2011-09

Developing a software model to assess a nation's capability to conduct sustained, offensive cyber warfare

McElheny, Aric L.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEVELOPING A SOFTWARE MODEL TO ASSESS A NATION'S CAPABILITY TO CONDUCT SUSTAINED, OFFENSIVE CYBER WARFARE

by

Brian D. Cummings
Aric L. McElheny

September 2011

Thesis Advisor: Raymond R. Buettner, Jr.
Co-Advisor: Dorothy E. Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Developing a Software Model to Assess a Nation's Capability to Conduct Sustained, Offensive Cyber Warfare		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Brian D. Cummings, Aric L. McElheny			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number_____N/A_____.			
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This research provides a Situational Influence Assessment Module (SIAM) software model for assessing the capability of a country to conduct sustained, offensive cyber warfare. The SIAM Cyber Warfare Capability Model identifies a process to quantify the baseline information needed to evaluate a complex problem. The model is a tool and allows analysts to understand the reasoning behind the assessments made by the model. The SIAM Cyber Warfare Capability Model is meant to be used as a mechanism to examine in detail the factors that should indicate a country's cyber warfare capabilities.

The SIAM Cyber Warfare Capability Model is a four level, hierarchical model that relies on user-defined relationships (links) to inform and assess whether a country has the capability to conduct, sustained offensive cyber warfare. The model requires the user provide a confidence value for the information contained within the Initial Nodes at the lowest level, level four, which will propagate up through the model based on user defined link strengths. The model accounts for the cumulative effect that multiple inputs may have on a nation state's cyber warfare capability through Causal Strengths (CAST) Logic. The analyst is also able to alter the information contained in the level four nodes along with the strength of the links, as more information is made available. This provides for a readily updateable model that considers multiple indicators and relationships.

The SIAM Cyber Warfare Capability Model required 15,010 evaluations in its design once the four level structure was adopted. During the development of the model, we constrained ourselves to work within the data considerations provided by the sponsor. The model requires the user to decide the relative importance of pertinent considerations, as defined within the model, when defining the level four Initial Nodes. The model becomes easily expandable if the analyst determines there is a key consideration missing for an Initial Node it can be incorporated and documented. Furthermore, the model is readily transferrable. The models link strengths and reasoning are well documented allowing for it to be applied to a variety of nations and utilized by multiple organizations.

The SIAM Cyber Warfare Capability Model was delivered to the sponsor, who then shared the model with other members of the Intelligence Community (IC). The sponsor endorsed the approach in our model and felt it provided a solid foundation for future modeling efforts. The sponsor used the Cyber Warfare Capability Model to account for resources in a separate model that analyzes a state's cyber program by taking a capability equals sophistication times resources approach. We view this feedback and subsequent use of our model in a separate product as a validation of the methodology employed in the Cyber Warfare Capability Model.

14. SUBJECT TERMS Computer Network Operations (CNO), Computer Network Defense (CND), Computer Network Exploitation (CNE), Computer Network Attack (CNA), Cyber Situational Influence Assessment Module (SIAM), Influence Net	**15. NUMBER OF PAGES** 85
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DEVELOPING A SOFTWARE MODEL TO ASSESS A NATION'S CAPABILITY TO CONDUCT SUSTAINED, OFFENSIVE CYBER WARFARE

Brian D. Cummings
Lieutenant, United States Navy
B.A., Ohio Dominican College, 1995

Aric L. McElheny
Lieutenant, United States Navy
B.S., United States Naval Academy, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2011

Authors: Brian D. Cummings

Aric L. McElheny

Approved by: Raymond R. Buettner, Jr.
Thesis Advisor

Dorothy E. Denning
Co-Advisor

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research provides a Situational Influence Assessment Module (SIAM) software model for assessing the capability of a country to conduct sustained, offensive cyber warfare. The SIAM Cyber Warfare Capability Model identifies a process to quantify the baseline information needed to evaluate a complex problem. The model is a tool and allows analysts to understand the reasoning behind the assessments made by the model. The SIAM Cyber Warfare Capability Model is meant to be used as a mechanism to examine in detail the factors that should indicate a country's cyber warfare capabilities.

The SIAM Cyber Warfare Capability Model is a four level, hierarchical model that relies on user-defined relationships (links) to inform and assess whether a country has the capability to conduct, sustained offensive cyber warfare. The model requires the user provide a confidence value for the information contained within the Initial Nodes at the lowest level, level four, which will propagate up through the model based on user defined link strengths. The model accounts for the cumulative effect that multiple inputs may have on a nation state's cyber warfare capability through Causal Strengths (CAST) Logic. The analyst is also able to alter the information contained in the level four nodes along with the strength of the links, as more information is made available. This provides for a readily updateable model that considers multiple indicators and relationships.

The SIAM Cyber Warfare Capability Model required 15,010 evaluations in its design once the four level structure was adopted. During the development of the model, we constrained ourselves to work within the data considerations provided by the sponsor. The model requires the user to decide the relative importance of pertinent considerations, as defined within the model, when defining the level four Initial Nodes. The model becomes easily expandable if the analyst determines there is a key consideration missing for an Initial Node, it can

be incorporated and documented. Furthermore, the model is readily transferrable. The models link strengths and reasoning are well documented allowing for it to be applied to a variety of nations and utilized by multiple organizations.

The SIAM Cyber Warfare Capability Model, was delivered to the sponsor, who then shared the model with other members of the Intelligence Community (IC). The sponsor endorsed the approach in our model and said it provided a solid foundation for future modeling efforts. The sponsor used the Cyber Warfare Capability Model to account for resources in a separate model that analyzes a state's cyber program by taking a capability equals sophistication times resources approach. We view this feedback and subsequent use of our model in a separate product as a validation of the methodology employed in the Cyber Warfare Capability Model.

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACM	Association for Computing Machinery
C2	Command and Control
CAST	Causal Strengths
CBA	Capabilities Based Assessment
CIA	U.S. Central Intelligence Agency
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COG	British Defense Cyber Operations Group
DHS	U.S. Department of Homeland Security
DI	British Defense Intelligence
DIA	U.S. Defense Intelligence Agency
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOTMLPF	Doctrine, Organization, Training, Materiel, Logistics, Personnel, Facilities
FBI	Fedral Bureau of Investigation
GCHQ	British Government Communications Headquarters
GDP	Gross Domestic Product
GRU	Russian Main Intelligence Directorate
HUMINT	Human Intelligence
IC	Intelligence Community
IEEE	Institute for Electrical and Electronics Engineers
INTERPOL	International Criminal Police Organization
IO	Information Operations
ISP	Internet Service Provider
ISSA	Information Systems Security Association
IT	Information Technology
ITU	International Telecommunications Union

IW	Information Warfare
MI5	British Secret Service
MI6	British Secret Intelligence Service
MSS	Chinese Ministry of State Security
NCSD	U.S. National Cyber Security Division
NPS	Naval Postgraduate School
NRI	Networked Readiness Index
NSA	U.S. National Security Agency
OPSEC	Operations Security
SIAM	Situational Influence Assessment Model
SIGINT	Signals Intelligence
ST&E	Science, Technology, and Engineering
SVR	Russian Foreign Intelligence Service
US-CERT	U.S. Computer Emergency Readiness Team
USCYBERCOM	U.S. Cyber Command

ACKNOWLEDGMENTS

We would like to express our sincere gratitude to both Dr. Ray Buettner and Dr. Dorothy Denning for their subject matter expertise, inspiration, support, and feedback throughout this whole process. We thank you both for your guidance and wisdom during this project.

From Brian: To my loving wife, Traci, and my two wonderful daughters, Shannon and Emily, thank you all for your patience and understanding during my work on this project. Without your support and tolerance, I would not have been able to complete this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The threat of foreign nation states conducting offensive cyber attacks against the United States is a National Security matter due to the ever-increasing reliance on information technologies in the modern world. This necessitates the ability to evaluate the offensive cyber capabilities possessed by a given nation. Nation states have the capability to leverage cyber capabilities with all source intelligence support, extensive resources, and potentially a kinetic attack to increase the level of impact. The potential effects of a cyber attack could be devastating if the United States is not prepared for them. Thus, in the ever-evolving threat environment, having an understanding of potential adversaries and their associated capabilities is the first step in defense. The capability to assess a nation state's sustained cyber capabilities is critical and has been recognized across the Intelligence Community. The research conducted and methodology employed is in support of a U.S. government agency in the intelligence community.

The ability to assess a nation state's offensive cyber capabilities, to include Computer Network Attack (CNA) and Computer Network Exploitation (CNE), is a high priority for the Intelligence Community (IC) as the national and military infrastructures are increasingly reliant on information technology. A consistent methodology for conducting such an assessment does not exist.

B. OBJECTIVES

This thesis will focus on developing a model for assessing whether a Nation State has sustainable offensive cyber capability.

The evaluation of a potential adversary's offensive Computer Network Operations (CNO) capabilities will be assessed using a Situational Influence Assessment Module (SIAM). The advantage of using SIAM is that for this work,

a model can be constructed that quantifiably identifies data points regarding the capacity for another nation state to launch a cyber attack. The ability to determine another nation state's capabilities would be very valuable if a conflict with the adversarial country ever broke out. Moreover, the model may help identify key warning indicators, and help focus limited resources in determining a target's sustained, offensive cyber capacity, potentially avoiding a strategic surprise.

The model does not address intent, and requires the analysts to have prerequisite knowledge of the target country. This thesis takes an overarching approach in the evaluation of key elements that effect cyber capabilities in order to help the analyst gain further understanding of the system being modeled, a nation state's cyber apparatus. The model helps develop a methodology in which a thorough evaluation of potential indicators is taken into account. The goal is to provide a baseline process of determining a nation state's cyber capabilities without completely overwhelming the analyst.

This thesis examines several factors that directly or indirectly contribute to a nation state's cyber capabilities. It is through this holistic approach, coupled with the knowledge of the analysts, that greater understanding of these capabilities is gained. This addresses a concern that there is a significant lack of net assessment concerning the trends in offensive CNO capacity. The Cyber Warfare Capability Model may be able to identify early warning indicators for offensive cyber capabilities. As a result, the analyst will be able to focus on key nodes and relationships, rather than having to determine exactly how a single factor impacts a complex system. The manner in which the model is defined may lead to new insights in how individual considerations fit into the overall assessment.

C. BRIEF EXPLANATION OF METHODOLOGY

This thesis is focused on assessing the offensive cyber capabilities of foreign nation states. This is done using a SIAM model that is based on Causal

Strengths (CAST) Logic. The SIAM Cyber Warfare Capability Model will provide a net assessment that takes a holistic approach examining policy, doctrine, technical ability, command and control, computer network infrastructure, facilities, and intelligence (Rosen & Smith, 1996). The Capablility Model is unique in that it integrates every element that is deemed significant, defines their relationships, and provides an assessment of the selected nation state's sustained CNA/CNE capacity. The advantage of using SIAM is that it will provide not only a net assessment, but also documentation for the underlying source material that is easily accessed by the analysts or end user. This information is available for the current decision makers and is readily updatable, capable of being refined in future assessments. Once causal relationships are effectively defined, and because all of the documentation is contained within, the Cyber Warfare Capability Model becomes a very powerful tool that can be transferred to different organizations and used by analysts at each.

D. THESIS STRUCTURE

Five chapters and three appendices comprise this thesis:

- *Chapter I—Introduction:* Establishes the goals for this thesis. Identifies the motivation and purpose behind conducting this research.
- *Chapter 2—Background:* Provides an overview of SIAM and the modeling process.
- *Chapter 3—Methodology:* Discusses the development and application of principles used to evaluate a Nation State's sustained offensive cyber capabilities. This fuses the academic world with real world analyst feedback and application.
- *Chapter 4—Cyber Warfare Capability Model:* This is a comprehensive look at the model and the categories that inform it.
- *Chapter 5—Conclusions and Recommendations:* Explains the conclusions and provides recommendation for future applications and research.
- *Appendix A—List of 79 Potential Considerations*: Lists the data an analyst should consider when populating the initial nodes of the model.

- *Appendix B—Mapping Considerations to Nodes*: Provides a quick reference table listing each node with the model and which considerations should be examined for each.
- *Appendix C—CNO Capability Model Guide*: A basic How-To guide for those not familiar with how SIAM works.

II. BACKGROUND

A. SITUATIONAL INFLUENCE ASSESSMENT MODULE (SIAM)

SIAM is a mature software tool that allows analysts and decision makers to simplify the analysis of complex issues using an influence net, which is a user-created model that depicts events and/or assumptions and their causal interrelationships. It provides users the capability to display issues graphically in order to view the complex cause-and-effect relationships and to easily manipulate or modify the events as new information becomes available (Figure 1). The software also provides comparative quantitative assessment techniques to evaluate the relative influencing impacts of the relationships (Science Applications International Corporation, 1995).

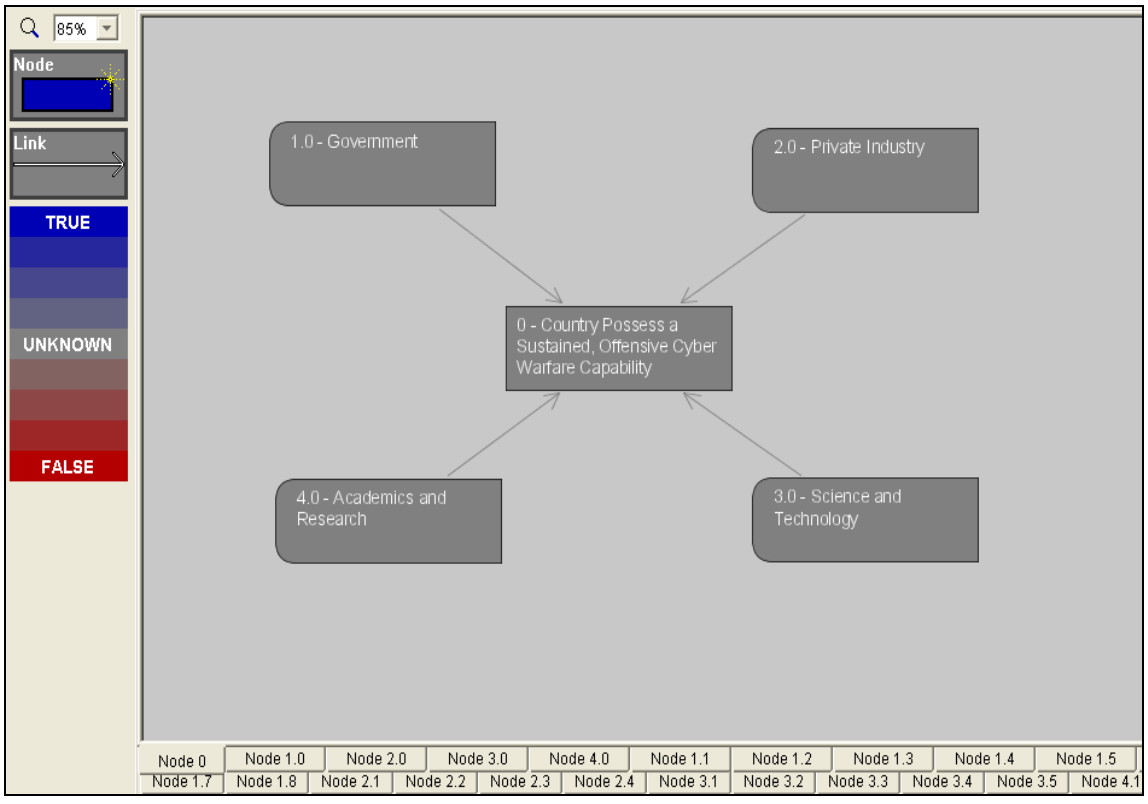

Figure 1. Graphic representation of the model

B. SIAM NODES

The basic elements of an influence net in SIAM are nodes and links. Nodes are the events, ideas, or assumptions that have an influence on the outcome of an overall issue. This issue or question to be evaluated by the SIAM model forms the Root Node of the influence network. The Root Node does not influence other events, but rather is the result of causal effects of the other nodes in the network. The SIAM Cyber Warfare Capability Model is a four-layered model, with the Root Node being the level 1 node. The other nodes are either Parent Nodes (causes) or Child Nodes (effects) and exist on lower layers. The lowest level of the model, level 4, consists of Initial Nodes, which are the primary assumptions in the model and are not influenced by any other nodes, only by the data entered by the user. All of the Initial Nodes function as Parent Nodes to the nodes that sit at level 3. The level 3 nodes are Internal Nodes that are between the Initial Nodes and the level 2 nodes. The level 3 Internal Nodes function as both Parent Nodes for the nodes that sit at level 2 and Child Nodes to the level 4 nodes. The level 2 nodes are Parent Nodes for the Root Node, but are Child Nodes to the level 3 nodes. Each node within the model is assigned a belief value, which is a statement as to the likelihood that the event represented by the node will occur or whether the assumption is true or false (Figure 2). Users set the belief values for the level four, Initial Nodes, manually because there is no information that SIAM can use to determine their beliefs based on influence. Belief values for Internal Nodes and Root Nodes are determined by SIAM based on the cumulative effect of all influencing nodes' belief values and the corresponding links' strengths (Rosen & Smith, 1996).

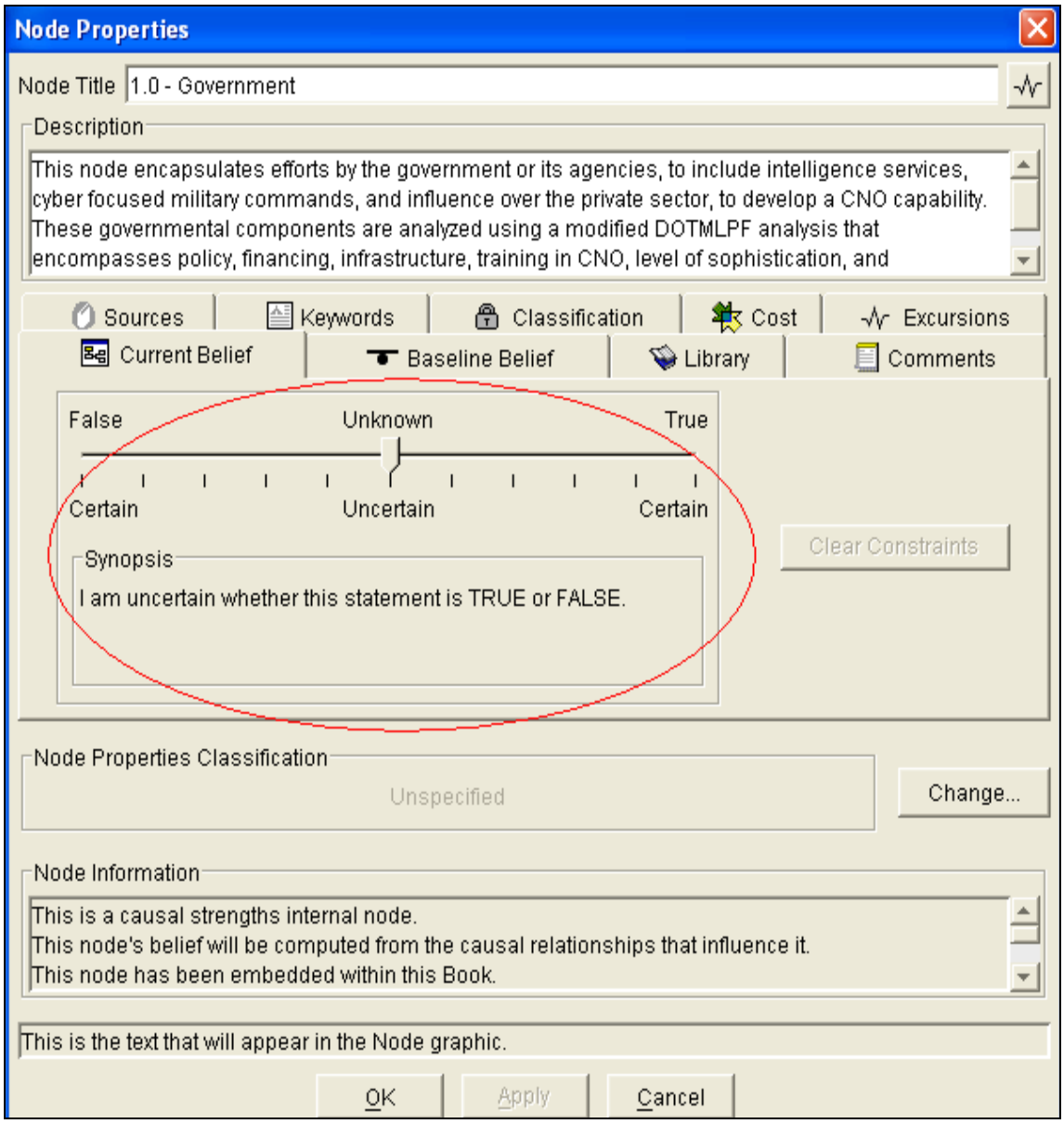

Figure 2. Belief value slider bar

C. SIAM LINKS

The other basic element of the influence net is the link, which is the representation of the causal relationship between Parent Nodes (causes) and Child Nodes (effects). The user assigns a strength value for each link within the influence net (Figure 3). This strength value represents the degree to which the

Parent Node influences the Child Node. Each link can have one of two influencing effects. A reinforcing influence means that, as the belief in the Parent Node increases, the belief in the Child Node also increases. A reversing influence means that, as the belief in the Parent Node increases, the belief in the Child Node decreases (Science Applications International Corporation, 1995).

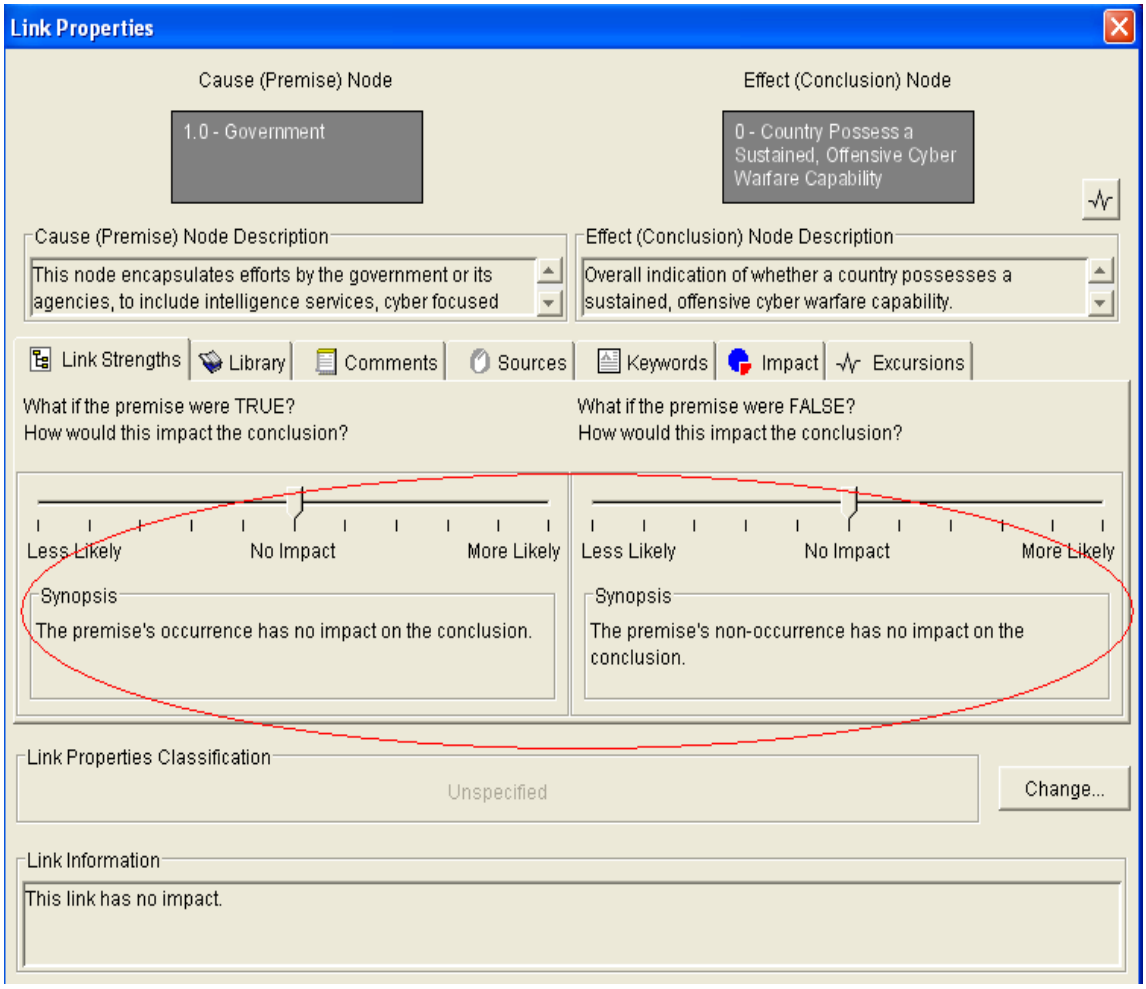

Figure 3. Link strength slider bars

D. SIAM BASICS

Once the user has assigned the belief values to the Initial Nodes and the strength values to the links, SIAM is ready to perform its comparative analysis. The analysis takes the belief value of the Initial Nodes together with the user-assigned link strengths to calculate the belief values of the Internal Nodes and a final assessment of the Root Nodes. SIAM uses the traditional influence net propagation algorithm based on Causal Strength (CAST) logic, which is a specific implementation of the more general class of Bayesian propagation algorithms. These types of algorithms are beneficial when the outcome is highly complex and cannot be modeled using static dependency logic rules. Bayesian algorithms account for the available information, as well as the potential lack of information about an event or an assumption. This allows for the evaluation of the cumulative effect that multiple causes may have on a single event (Rosen & Smith, 1996).

E. BENEFITS OF SIAM ANALYSIS

Analyzing a complex issue or answering a complex question can be a largely nonintuitive task where the analyst must consider a large amount of data, much of which, when considered individually, provides little insight into the final assessment of the issue. The more complex the issue or question, the more likely the individual factors affecting the outcome are going to be vague and contribute less. Crucial to the analysis is determining which of the many pieces of data are important, and understanding the corresponding relationships. SIAM simplifies this process by providing the user with a set of tools that allow for easy organization and documentation of large amounts of information, visualization of the strength of relationships between causes and effects, and identification of elements where the model is lacking sufficient information. Most importantly, however, is the ability for SIAM to identify the causal elements with the greatest chance to affect the overall outcome (Science Applications International Corporation, 1995). With these so-called pressure nodes identified, analysts

know where to focus limited resources for information collection and further analysis, and decision makers know where to employ capabilities in order to obtain the desired outcome—allocating the appropriate resources to the right event at the right time.

III. METHODOLOGY

A. ACADEMIC REVIEW

The approach taken in the development of the Cyber Warfare Capability Model was driven by academic research as well as sponsor needs. An academic review of previous work in the field was conducted to understand the process other scholars had taken in considering CNO capabilities. Our work is heavily influenced by previous work conducted at the Naval Postgraduate School (NPS) in 2004–2005 on the CNO threat of foreign countries. That work, which was supervised by Dr. Dorothy Denning and conducted by Lieutenants Christopher Brown, Jason Patterson and Matthew Smith, focused on developing a reliable methodology of assessing the CNO threat of foreign countries (Denning, 2007). The methodology grouped indicators of CNO capabilities into four categories:

- Information technology industry and infrastructure
- Academic and research community
- Government and foreign relations
- Hacking and cyber attacks

The study played a large role in shaping our early perceptions regarding CNO threats and led us to realize that the presence of a computer network defense (CND) capability may correspond with some CNA or CNE capability. While CNE/CNA require a different application of knowledge, it is undoubtedly related to CND. Essentially, knowledge of how systems are attacked is strongly correlated to building strong defenses. Thus, CND can be used as an indicator as it implies a certain level of knowledge regarding CNA/E, even if it has not been displayed. This approach is accounted for and incorporated into our own

research. The methodology employed by our research was a categorical approach and grouped indicators into four major classes:

- Government
- Private Industry
- Science and Technology
- Academics and Research

Additionally, we drew heavily upon the research conducted by the Institute for Security Technology Studies at Dartmouth College (Billo & Chang, 2004). The Dartmouth group focused on categorizing indicators into two sections. Category one consisted of direct links to cyber warfare capabilities, while category two was based on indirect links and circumstantial evidence such as the IT infrastructure (Billo & Chang, 2004). The Cyber Warfare Capability Model captures direct links as well secondary considerations; however, it relies on the analyst to determine the level of influence exerted. This will be explained further in the next section.

Both studies provided significant insight, which we used as a baseline for thinking about the CNO capabilities of a foreign country. The studies were conducted using real countries and source data, which provided further validation to these approaches. The real breakthrough in the previous studies was not the result of the information obtained, but rather the methodology employed. Both the NPS and Dartmouth studies provided invaluable insights in how to think about CNO. Neither, however, attempted to quantify their assessments of the countries they examined. This is where the Cyber Warfare Capability Model differs from previous work and provides a distinct contribution. The SIAM model provides a means of making a quantifiable assessment of a country's cyber capabilities as well as identifying the pressure points or key enablers of those capabilities.

B. DOTMLPF ANALYSIS

We met with the sponsor to discuss the approach we were considering for the Cyber Warfare Capability Model. The sponsor, while appreciating the approach, envisioned a level of analysis much deeper than just looking at the model from a categorical perspective. The sponsor wanted a model that would direct the analysts to answer the question: *Does said Nation State have the capability to conduct sustained, offensive cyber warfare*?

The sponsor suggested using a modified DOTMLPF approach. DOTMLPF Analysis identifies possible nonmateriel solutions as a result of a capabilities-based assessment (CBA) to satisfy a capability gap (Chairman of the Joint Chiefs of Staff, 2011). The modified DOTMLPF analysis considered cyber related factors, tweaking the traditional approach of DOTMLPF: doctrine, organization, training, materiel, leadership and education, personnel, and facilities. We combined the categorical methodology with a DOTMLPF Analysis in a hierarchal model to take an all-inclusive approach to determining whether a CNO capacity exists. The categories exist on the second level of the model and are composed of sectors (objects) for consideration on level three. Each sector is then analyzed using the modified DOTMLPF Analysis at level four. The cumulative effect of the analysis is propagated through the model based on Initial Nodes and link strengths assigned by the analysts. The following is a breakdown of the modified DOTMLPF Analysis which are each represented by Initial Nodes on level 4:

- *Doctrine*: The fundamental principles that guide the employment of forces in coordinated action toward a common objective.
- *Organization*: A unit with varied functions enabled by a structure through which individuals cooperate systematically to accomplish a common mission and directly provide or support mission capabilities.
- *Training and Education*: Training based on doctrine or tactics, techniques, and procedures to prepare forces or staffs to respond to strategic and operational requirements deemed necessary by

leaders to execute their assigned missions; how we prepare to fight.

- *Materiel*: All items necessary to equip, operate, maintain, and support units without distinction as to its application for administrative or operational purposes.
- *Financing:* The level of financial support afforded to the organization to enable the other aspects of the DOTMLPF paradigm to mature.
- *Personnel*: availability of qualified people for peacetime, wartime, and various contingency operations.
- *Facilities*: real property; installations and industrial facilities that support cyber forces.
- *Research and Development:* Creative work undertaken on a systematic basis in order to increase the stock of knowledge, and the use of this knowledge to devise new applications.
- *Sophistication:* The level to which the capability has progressed in complexity and maturity.
- *Support to Cyber Operations:* The actions of an organization that aid, protect, complement, or sustain a unit conducting cyber operations.

The modified DOTMLPF Analysis enables a systems engineering approach to be taken in determining whether a country has a CNO capacity. Systems engineering is a top-down process of transforming requirements into an integrated solution. The modified DOTMLPF Analysis is a very structured technique that forces the analyst to examine the problem from a multitude of angles. The Cyberwarfare Capability Model accounts for dynamic variables in a quantifiable manner to meet the functional requirements of the sponsor.

C. MODEL STRUCTURE (OBJECTS/TRAITS/CONSIDERATIONS)

The Cyberwarfare Capability Model is a four level model that requires the analysts to define all relationships. The analysts will provide data to the Initial Nodes at the lowest level, level four, which will propagate through the model and determine whether a country has the capacity to conduct sustained, offensive cyber operations. Collaborating with the sponsor, an object-traits-considerations

framework was adopted to meet the objectives of the model. The Root Node, which exists on level 1, is the question being evaluated by the model (Node 0– Country Possess a Sustained, Offensive Cyber Warfare Capability). The SIAM model will account for the relative certainty that a country possesses the capability to conduct sustained, offensive cyber warfare based on the lower level nodes and link relationships. The level of a country's cyber warfare capability is directly linked to the sophistication of said capability. Sophistication is addressed in the model as part of the modified DOTMLPF Analysis, informing the level 3 objects. The categories exist at level 2 and act as Parent Nodes to the Root Node by feeding information into level 1 node to determine whether a country possesses a sustained CNA capability (Figure 4). The categories, defined in the Section A of this chapter, are Child Nodes to the level 3 nodes. The level 3 nodes are Internal Nodes, as well, and consist of objects contained within the four distinct level 2 categories. Each category (level 2) consists of distinct objects (level 3) that contribute to a sector of the country's ability to conduct sustained CNA activities (Figure 5). The objects are Parent Nodes to the categories and inform them as such. The model will require the analyst to determine the significance of the relationship between each node, as the influence that a node exerts could be target specific. The amount of influence each object has is determined by the link strengths the analyst assigns between the level 1, level 2, and level 3 nodes. However, the model presents a structured manner for the analyst to think about the problem as every object undergoes a modified DOTMLPF Analysis.

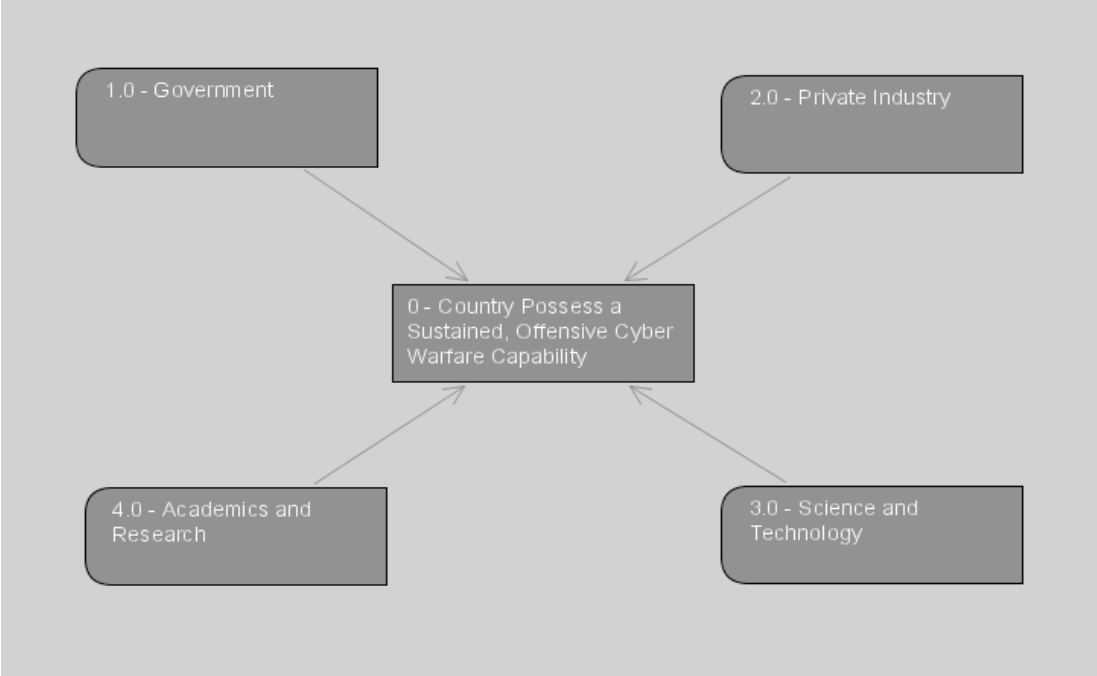

Figure 4. Level 2 categories

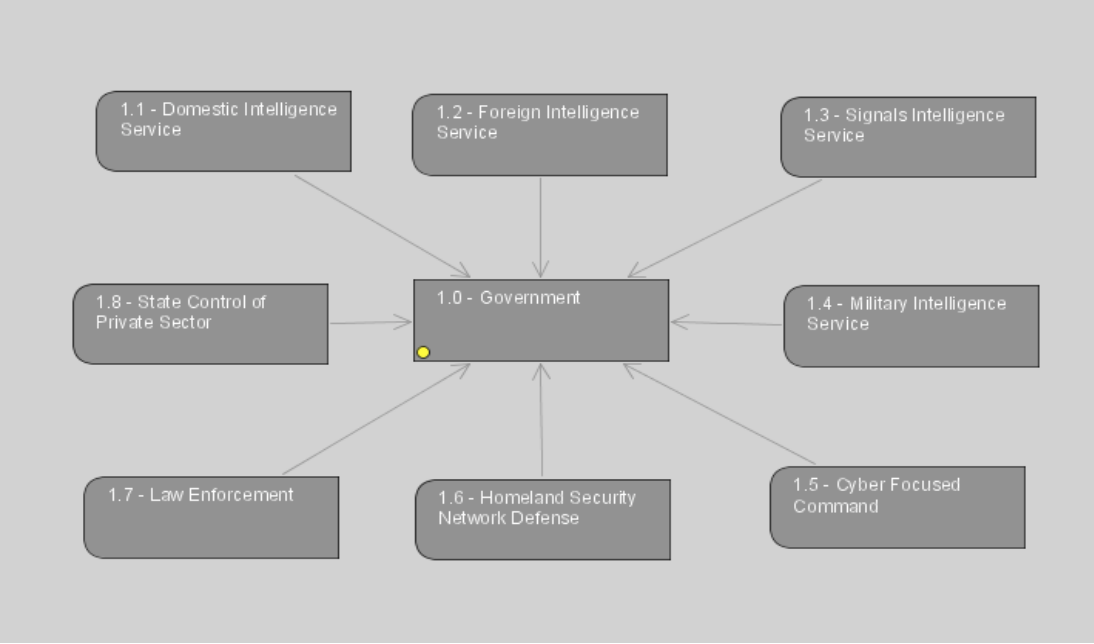

Figure 5. Level 3 objects

The Initial Nodes are at the lowest level, level 4, and represent the traits, which make up the modified DOTMLPF Analysis. Each object is a Child Node to the level 4 nodes, as each undergoes a modified DOTMLPF Analysis. This means that each object has 10 Parent/Initial Nodes influencing it. The Initial Nodes (traits) are informed by considerations, contained within the Initial Nodes comments. There are 79 potential considerations that were considered when developing this model. A thorough evaluation of all 79 potential considerations was conducted and as a result each trait (Initial Node) is assigned applicable considerations for the analyst to account for when assigning a belief value to the node (Figure 6).

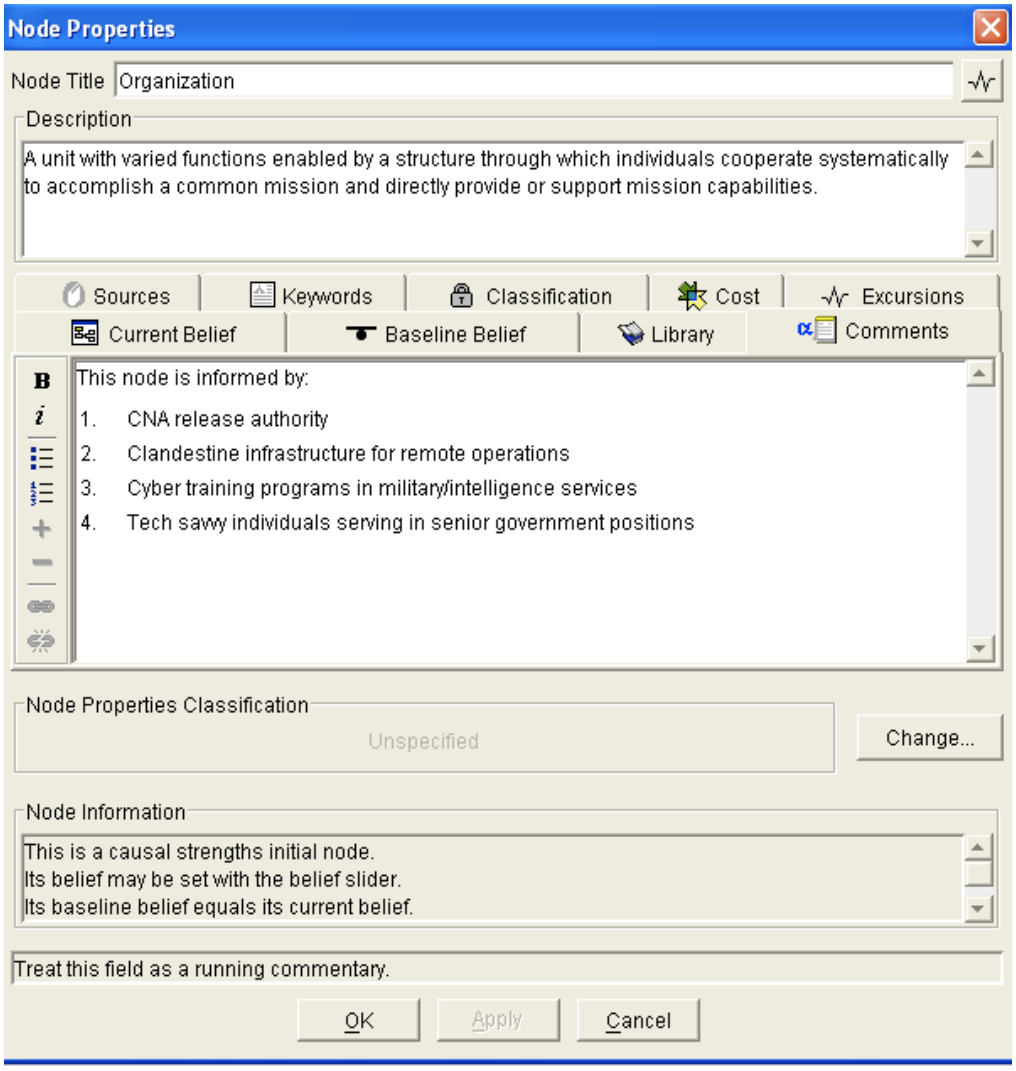

Figure 6. Informing considerations

The model requires the analyst to evaluate the considerations multiple times in the Initial Nodes. This decision was made as a result of software design constraints. It would have been ideal for the analyst to just assign a value to each of the 79 considerations once and let those values flow through the model. However, this would not be graphically manageable and would overwhelm the analyst as a result. The layered design employed has two benefits. First, the model is manageable for the analyst, as everything is categorized in a hierarchal manner. The analyst is easily able to resolve inputs and see the correlation to the model. Second, a consideration may have a different weight when considering disparate traits. Further, the model becomes easily expandable if the analyst determines there is a key consideration missing for a level-4 trait (Initial Node), he/she can simply add it in and document it.

IV. CYBER WARFARE MODEL

To begin, we considered the main factors that would influence a nation's capability to conduct sustained, offensive cyber warfare. This was considered strictly from the standpoint of a nation state. The ability to conduct cyber warfare by groups other than actual nations (i.e., transnational criminal organizations, terrorists, amateur hackers and hacktivists) was not formally examined. However, in some instances, a nation's ability to conduct cyber warfare depends heavily upon leveraging the talents of the above mentioned groups, so the model takes this into consideration at various points. In considering the question at the nation state level, we determined the four main influences were government, private industry, science and technology, and academics and research (Figure 7).

The modified DOTMLPF Analysis was used in analyzing each of the four main node families (level 2 nodes) by applying it to each object (level 3 node). This chapter highlights the key traits (level 4 nodes) for each object (level 3 node) based on the criterion that it contained the most considerations for the analyst to deliberate. The model accounts for the full allocation of traits for each object, and the analyst has the ability to emphasize or deemphasize the traits' importance by assigning link strengths. The considerations can be direct or indirect influences to the traits they inform. It should be noted that this is a gray model, meaning that none of the link strengths nor the initial node belief values have been assigned. Based upon discussions with the sponsor, it was decided that this information would vary from country to country and an accurate assignment of link strengths and node belief values should be conducted on a country-by-country basis by the analyst familiar with that particular data set. That way the analyst has the ability to decide the relative importance of the various factors for each country. The Cyber Warfare Capability Model provides a systematic process for the analyst to approach the problem. This chapter discusses in detail the analysis of each of these four families of nodes (level-2

nodes) and how they ultimately influence the root node of whether a country possesses a sustained, offensive cyber warfare capability.

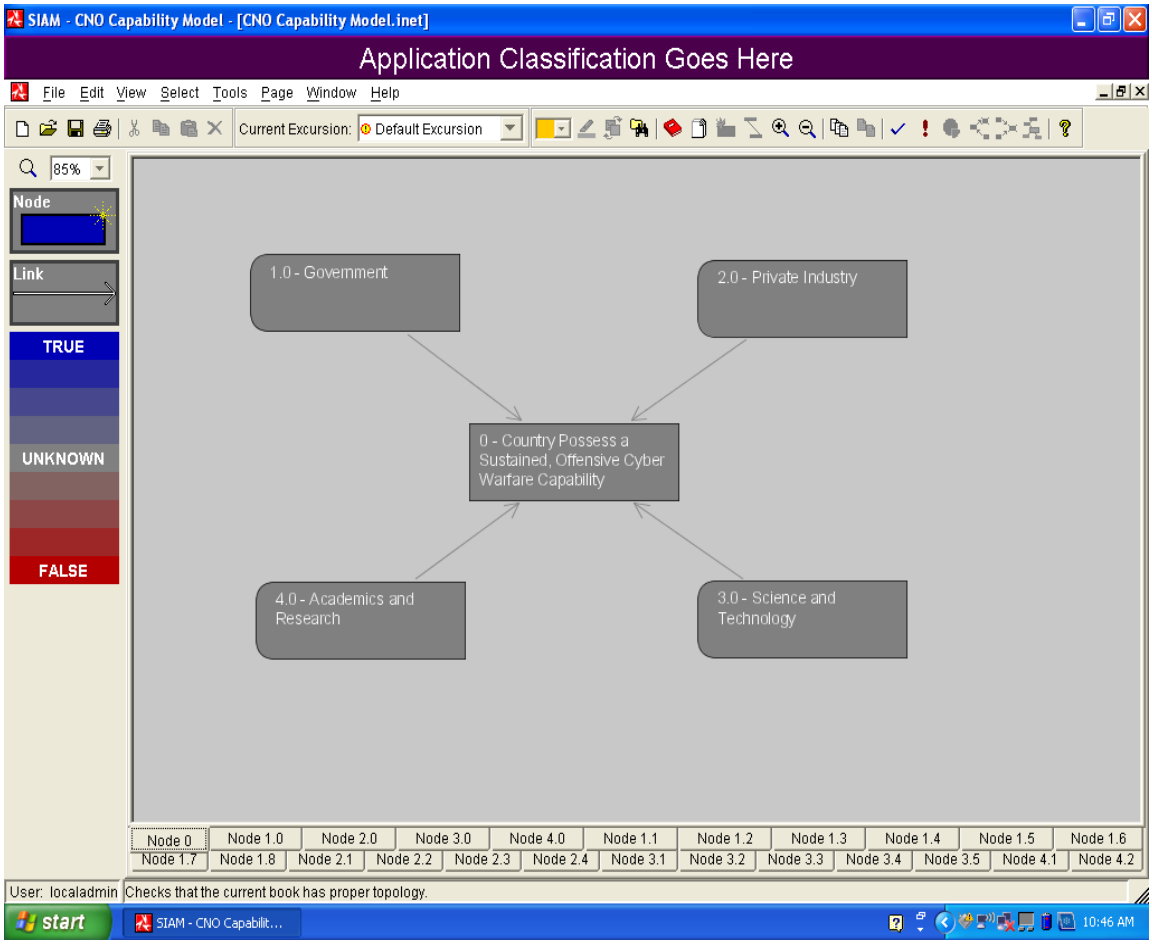

Figure 7. Top level of Cyber Warfare Capability Model

A. GOVERNMENT

Acknowledging that the Cyber Warfare Capability Model considers the root question from the standpoint of a nation state, it is understandable that the largest node family is that of government. This node encapsulates the efforts by the government or its agencies to develop and maintain a sustained, offensive cyber warfare capability. The government node has eight parent nodes—nodes that have a causal influence on the government node (Figure 8). These influences are the domestic intelligence service, the foreign intelligence service,

the signals intelligence service, the military intelligence service, a cyber-focused military command, homeland security network defense, law enforcement, and state control over the private sector.

The most robust parent nodes within this family are the foreign intelligence service and the signals intelligence service, followed by a cyber-focused military command and homeland security network defense. For a cyber warfare capability to be effective and efficient, a nation needs timely and accurate intelligence on its foreign adversaries and their networks. Without effective foreign and signals intelligence services, the ability to conduct sustained, offensive cyber warfare will diminish greatly. The U.S. Department of Defense (DoD) defines intelligence as the product resulting from collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations (Department of Defense, 2011). In his work for the Central Intelligence Agency (CIA) Center for the Study of Intelligence, Rob Johnston defined intelligence as a secret state or group activity to understand or influence foreign or domestic entities (Johnston, 2005). In the case of cyber warfare, the state would be the group conducting the intelligence and the foreign entities networks would be those that the state were trying first to understand, and then influence.

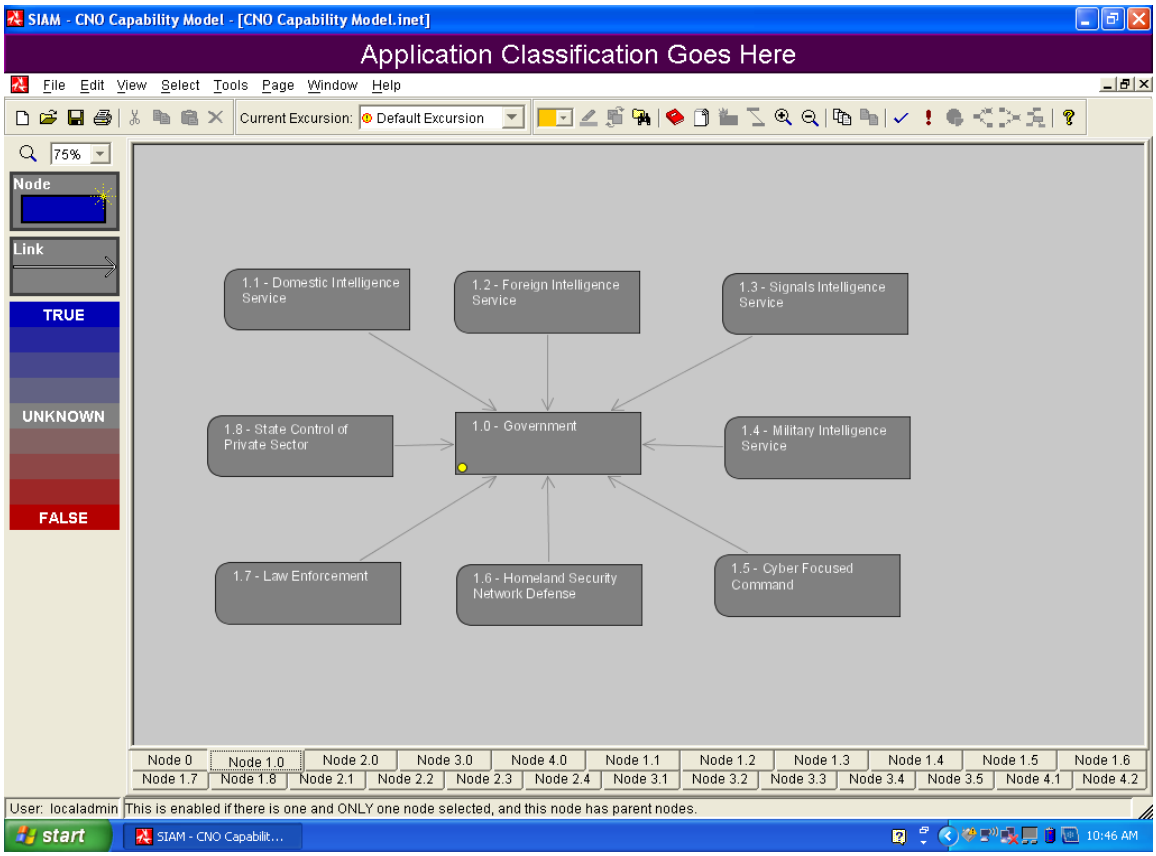

Figure 8. Government node of the Cyber Warfare Capability Model

1. Domestic Intelligence Service

This node represents the presence of a domestic intelligence service, similar to the United States Federal Bureau of Investigation (FBI), the British Security Service (MI5), the Israeli Shin Bet, the Russian Federal Security Service (FSB), or the Chinese Ministry of State Security (MSS). The definition of domestic intelligence is intelligence relating to the activities or conditions inside a country that threaten that country's security (Department of Defense, 2011). For example, the FBI produces intelligence in support of its own investigative mission, national intelligence priorities and the needs of other customers (Federal Bureau of Investigation). While the primary mission of the FBI is U.S. federal law

enforcement, the intelligence gathered during their investigative operations undoubtedly aids the overall national cyber warfare mission, both offensively and defensively ("FBI Warns," 2010).

The domestic intelligence node is most heavily influenced by the traits of doctrine, facilities, sophistication and support to cyber operations. In the model, when determining how each of the traits influences the domestic intelligence service and its support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Doctrine**: (1) the level of state control of the tech sector, (2) the relationships between the government/intelligence services and the nation's domestic corporations, (3) any operations against domestic opposition websites, (4) the level of concern over cybercrime and, (5) the overall information warfare (IW) program operations security (OPSEC) level.
- **Facilities**: (1) the midpoint SIGINT capability, (2) the covert communications capability, (3) the capability to create and run front companies and, (4) the number of classified networks in the government information technology (IT) infrastructure.
- **Sophistication**: (1) the acquisition of black market cyber tools, (2) the sophistication of the human intelligence (HUMINT) program, (3) the midpoint SIGINT capability, (4) the covert communications capability, (5) the capability to steal technology and make use of it outside of cyber operations, (6) the overall intelligence collection capabilities not related to cyber operations and, (7) the capability to remotely delete data from websites or computers.
- **Support to Cyber Operations**: (1) the acquisition of black market cyber tools, (2) the midpoint SIGINT capability, (3) the relationships between government/intelligence services and the nation's domestic corporations and, (4) the capability to remotely delete data from websites or computers.

2. Foreign Intelligence Service

This node represents the presence of a foreign intelligence service, similar to the United States (CIA), the British Secret Intelligence Service (MI6), the Israeli Mossad, the Russian Foreign Intelligence Service (SVR), or the Chinese MSS. The definition of foreign intelligence is information relating to the

capabilities, intentions, and activities of foreign powers, organizations, or persons (Department of Defense, 2011). Having an effective foreign intelligence service is vital for an effective cyber warfare capability. Cyberspace is the newly recognized fifth domain of warfare (along with air, land, sea, and space) ("Cyberwar," 2010). Perhaps more than any other domain of warfare, cyberspace requires detailed intelligence of the network infrastructure used by the adversary's decision makers. A nation's foreign intelligence service is the organization best suited to collect and analyze this information, providing the signals intelligence service with leads for thorough technical exploitation. As a recognized domain of warfare, the same rules apply for conducting warfare there. Without the necessary intelligence on the foreign networks, a cyber warfare capability could not exist.

The foreign intelligence node is most heavily influenced by the traits of doctrine, organization, materiel, facilities, personnel, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences the foreign intelligence service and its support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Doctrine**: (1) the relationships with other cyber actors, (2) the strength of nationalism in the population, (3) the relationships between the government/intelligence services and the nation's domestic corporations, (4) whether any covert cyber activity has been detected, (5) diplomatic cyber initiatives and, (6) the overall IW program OPSEC level.
- **Organization**: (1) who has CNA release authority, (2) the clandestine infrastructure for remote operations, (3) the cyber training programs in the military/intelligence services and, (4) whether there are technologically savvy individuals serving in senior government positions.
- **Materiel**: (1) the covert communications capability, (2) any observation of traveling government IT technicians servicing information operations platforms abroad, (3) the clandestine infrastructure for remote operations, (4) the number of classified networks in the government IT infrastructure and, (5) any evidence of storage for massive amounts of collected cyber data.

- **Facilities**: (1) the number of intelligence bases internationally, (2) the midpoint SIGINT capability, (3) the covert communications capability, (4) the clandestine infrastructure for remote operations, (5) the number of classified networks in the government IT infrastructure and, (6) any evidence of storage for massive amounts of collected cyber data.
- **Personnel**: (1) the linguistic capability, (2) the size of the hacker community, (3) the strength of nationalism in the population, (4) the number of cyber related contracts for bid, (5) any observation of travelling government IT technicians servicing information operations platforms abroad and, (6) whether there are technologically savvy individuals serving in senior government positions.
- **Sophistication**: (1) the acquisition of black market cyber tools, (2) the sophistication of the HUMINT program, (3) the midpoint SIGINT capability, (4) the covert communications capability, (5) the capability to steal technology and make use of it outside of cyber operations, (6) the overall intelligence collection capability not related to cyber operations, (7) the capability to remotely delete data from websites or computers, (8) any documented CNE successes and, (9) the undersea cable operations capability.
- **Support to Cyber Operations**: (1) acquisition of black market cyber tools, (2) the size of the hacker community, (3) the sophistication of the HUMINT program, (4) the midpoint SIGINT capability, (5) the relationships between the government/intelligence services and the nation's domestic corporations, (6) any covert cyber activity detected, (7) the observation of traveling government IT technicians servicing information operations platforms abroad, (8) the capability to remotely delete data from websites or computers, (9) any document CNE successes, (10) diplomatic cyber initiatives and (11) the undersea cable operations capability.

3. Signals Intelligence Service

This node represents the presence of a signals intelligence (SIGINT) service, similar to the United States National Security Agency (NSA), the British Government Communications Headquarters (GCHQ), the Israeli Intelligence Corps Unit 8200, the Russian FSB, or the Chinese Third and Fourth Departments of the General Staff. SIGINT is defined as intelligence derived from communications, electronic, and foreign instrumentation signals (Department of

Defense, 2011). It is most likely through its SIGINT service that a nation conducting sustained, offensive cyber warfare will operate. Resident here will likely be the technical expertise required to develop the understanding of the adversary network topology and operating systems for reconnaissance, exploitation and eventually attack.

The signals intelligence node is most heavily influenced by the traits of doctrine, organization, materiel, facilities, research and development, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences the signals intelligence service and its support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Doctrine**: (1) the level of state control of the tech sector, (2) the relationships with other cyber actors, (3) the role that information operations plays across the spectrum of conflict, (4) the use of offensive CNO to support operations outside of strategic information operations, (5) the relationships between the government/intelligence services and the nation's domestic corporations, (6) any covert cyber activity detected, (7) any operations against domestic opposition websites, (8) any diplomatic cyber initiatives and, (9) overall IW program OPSEC level.
- **Organization**: (1) the presence of an information operations range infrastructure, (2) who has CNA release authority, (3) the clandestine infrastructure for remote operations, (4) any evidence of an Internet monitoring program, (5) the cyber training programs in the military/intelligence services and, (6) whether there are technologically savvy individuals serving in senior government positions.
- **Materiel**: (1) the presence of an IO range infrastructure, (2) the covert communications capability, (3) the level of botnet activity, (4) any observation of traveling government technicians servicing IO platforms abroad, (5) the clandestine infrastructure for remote operations, (6) the number of classified networks in the government IT infrastructure, (7) any evidence of storage for massive amounts of collected cyber data and, (8) a ranking in the top 100 of the world's fastest computers.
- **Facilities**: (1) the number of intelligence bases internationally, (2) the presence of an IO range infrastructure, (3) the midpoint SIGINT capability, (4) the technological sophistication of the population, (5)

the covert communications capability, (6) the clandestine infrastructure for remote operations, (7) the number of classified networks in the government IT infrastructure and, (8) any evidence of storage for massive amounts of collected cyber data.

- **Research and Development**: (1) the acquisition of black market cyber tools, (2) the presence of an information operations IO range infrastructure, (3) the capability to steal technology and make use of it outside of cyber operations and, (4) the relationships between the government/intelligence services and the nation's domestic corporations.
- **Sophistication**: (1) the acquisition of black market cyber tools, (2) the presence of an IO range infrastructure, (3) the midpoint SIGINT capability, (4) the presence of Silicon Valley-like high tech corridors, (5) the use of offensive CNO to support programs outside of strategic IO, (6) the covert communications capability, (7) the capability to steal technology and make use of it outside of cyber operations, (8) the overall intelligence collection capability not related to cyber operations, (9) the capability to remotely delete data from websites or computers, (10) any documented CNE successes and, (11) the undersea cable operations capability.
- **Support to Cyber Operations**: (1) the acquisition of black market cyber tools, (2) the presence of an IO range infrastructure, (3) the midpoint SIGINT capability, (4) the presence of Silicon Valley-like high tech corridors, (5) the role that IO plays across the spectrum of conflict, (6) the relationships between the government/intelligence organizations and the nation's domestic corporations, (7) any covert cyber activity detected, (8) the observation of traveling government technicians servicing IO platforms abroad, (9) the capability to remotely delete data from websites or computers, (10) evidence of a network mapping program, (11) any documented CNE successes, (12) evidence of an Internet monitoring program, (13) a ranking in the top 100 of the world's fastest computers, (14) any diplomatic cyber initiatives and, (15) the undersea cable operations capability.

4. Military Intelligence Service

This node represents the presence of a national level military intelligence service, similar to the United States Defense Intelligence Agency (DIA), the British Defense Intelligence (DI), the Israeli Aman, the Russian Main Intelligence Directorate (GRU), or the Chinese Second Department of the General Staff.

Military intelligence is defined as intelligence on any foreign military or military-related situation or activity, which is significant to military policymaking or the planning and conduct of military operations and activities (Department of Defense, 2011). Cyber warfare, as with any form of warfare, is conducted to gain some form of strategic or operational advantage. If cyber warfare is used as an enabler in conjunction with other, more traditional forms of warfare, then attacking the command and control (C2) networks of an adversary is a likely course of action. To gain the desired effects, a nation must have detailed knowledge of their adversary's military structure—the command relationships, force disposition and location, and C2 network. The role of military intelligence is to ensure this information is accurate so the cyber warfare actions are effective and the desired strategic or operational advantage is attained.

The military intelligence node is most heavily influenced by the traits of materiel, facilities, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences the military intelligence service and its support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Materiel**: (1) the number of classified networks in the government IT infrastructure, (2) evidence of storage for massive amounts of collected cyber data and, (3) evidence of power needed to support cyber facilities.
- **Facilities**: (1) the number of intelligence bases internationally, (2) the midpoint SIGINT capability, (3) the number of classified networks in the government IT infrastructure, (4) evidence of storage for massive amounts of collected cyber data and, (5) evidence of power needed to support cyber facilities.
- **Sophistication**: (1) the acquisition of black market cyber tools, (2) the sophistication of the HUMINT program, (3) the midpoint SIGINT capability and, (4) the overall intelligence collection capability not related to cyber operations.
- **Support to Cyber Operations**: (1) the acquisition of black market cyber tools, (2) the sophistication of the HUMINT program, (3) the midpoint SIGINT capability and, (4) any diplomatic cyber initiatives.

5. Cyber Focused Command

This node represents the presence of a military organization devoted to computer network operations (CNO), similar to the United Stated Cyber Command (USCYBERCOM), the British Defense Cyber Operations Group (COG), or the Israeli Unit 8200. Although not every country possessing an offensive cyber warfare capability has such a military command, the presence is a very strong indicator. It would represent significant investment in time, personnel and resources that could only indicate that nation's belief in the utility of developing and maintaining a sustained, offensive cyber warfare capability.

The cyber focused command node is most heavily influenced by the traits of doctrine, organization, materiel, facilities, personnel, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences the cyber focused command and its support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Doctrine**: (1) relationships with other cyber actors, (2) the strength of nationalism in the population, (3) sponsorship/participation in cyber security conferences, (4) the role that IO plays across the spectrum of conflict, (5) the use of offensive CNO to support programs outside of strategic IO, (6) any covert cyber activity detected, (7) a declaratory response policy, (8) operations against domestic opposition websites, (9) any diplomatic cyber initiatives and, (10) the overall IW program OPSEC level.
- **Organization**: (1) the presence of an IO range infrastructure, (2) open source reorganizations of IO organizations, (3) CNA release authority, (4) a clandestine infrastructure for remote operations, (5) cyber training programs in the military/intelligence services and, (6) technologically savvy individuals serving in senior government positions.
- **Materiel**: (1) the presence of an IO range infrastructure, (2) observation of traveling government IT technicians servicing IO platforms abroad, (3) a clandestine infrastructure for remote operations and, (4) the number of classified networks in the government IT infrastructure.
- **Facilities**: (1) the presence of an IO range infrastructure, (2) a clandestine infrastructure for remote operations, (3) the number of

classified networks in the government IT infrastructure and, (4) evidence of power needed to support cyber facilities.

- **Personnel**: (1) the strength of nationalism in the population, (2) the number of cyber related contracts for bid, (3) the recruiting of students to act as cyber operators, (4) observation of traveling government IT technicians servicing IO platforms abroad, (5) cyber training programs in the military/intelligence services and, (6) technologically savvy individuals serving in senior government positions.
- **Sophistication**: (1) the acquisition of black market cyber tools, (2) the presence of an IO range infrastructure, (3) the use of offensive CNO to support programs outside of strategic IO and, (4) any documented CNE successes.
- **Support to Cyber Operations**: (1) the acquisition of black market cyber tools, (2) the size of the hacker community, (3) the presence of an IO range infrastructure, (4) sponsorship/participation in cyber security conferences, (5) the role that IO plays across the spectrum of conflict, (6) any covert cyber activity detected, (7) observation of traveling government IT technicians servicing IO platforms abroad, (8) any documented CNE successes and, (9) any diplomatic cyber initiatives.

6. Homeland Security Network Defense

This node represents the presence of a national level agency dedicated to the protection of government networks, similar to the United States Department of Homeland Security (DHS), National Cyber Security Division (NCSD). Although not directly involved in offensive cyber warfare, an organization dedicated to protecting the nation's critical network infrastructure should give insight into how seriously a nation views cyber warfare. Also important is the fact that to effectively defend your network against attacks, you must first have a thorough understanding of the attack tools and methods. Therefore, effective defense means detailed knowledge of attack. As stated by Dr. Dorothy Denning of the NPS, "A country with a strong CND capability would be in a much better position to build and use a CNA/E capability than one without" (Denning, 2007).

The homeland security network defense node is most heavily influenced by the traits of doctrine, organization, materiel, personnel, and support to cyber

operations. In the model, when determining how each of the traits influences homeland security network defense and its support to the overall cyber warfare capability, the analyst should analyze the listed considerations.

- **Doctrine**: (1) relationships with other cyber actors, (2) the cybercrime level, (3) relationships with international cyber security organizations, (4) sponsorship/participation in cyber security conferences, (5) the capability to implement best practices in regards to computer security, (6) access to computer security data from international organizations (INTERPOL, ITU, etc.), (7) any diplomatic cyber initiatives and, (8) the overall IW program OPSEC level.
- **Organization**: (1) the presence of an IO range infrastructure, (2) open source reorganizations of IO organizations, (3) evidence of an Internet monitoring program, (4) a critical infrastructure protection program and, (5) technologically savvy individuals serving in senior government positions.
- **Materiel**: (1) the presence of an IO range infrastructure, (2) observation of traveling government IT technicians servicing IO platforms abroad, (3) the capability to implement best practices in regards to computer security and, (4) the number of classified networks in the government IT infrastructure.
- **Personnel**: (1) the number of cyber related contracts for bid, (2) the recruiting of students to act as cyber operators, (3) observation of traveling government IT technicians servicing IO platforms abroad and, (4) technologically savvy individuals serving in senior government positions.
- **Support to Cyber Operations**: (1) the presence of an IO range infrastructure, (2) sponsorship/participation in cyber security conferences, (3) observation of traveling government IT technicians servicing IO platforms abroad, (4) evidence of an Internet monitoring program, (5) any diplomatic cyber initiatives and, (6) the overall IW program OPSEC level.

7. Law Enforcement

This node represents law enforcement agencies at all levels of government that contribute to the enforcement of computer related crimes. During the course of investigation of crimes, particularly computer crimes, various law enforcement agencies will develop information regarding attack

signatures, tactics and potentially the origin of the attack, all of which is useful to other departments and agencies, specifically those focused on cyber warfare.

The law enforcement node is most heavily influenced by the traits of doctrine and sophistication. In the model, when determining how each of the traits influences law enforcement and its support to the overall cyber warfare capability, the analyst should focus on the listed considerations.

- **Doctrine**: (1) relationships with other cyber actors, (2) the cybercrime level, (3) access to computer security data from international organizations (INTERPOL, ITU, etc.), (4) operations against domestic opposition websites, (5) the level of concern over cybercrime, (6) any diplomatic cyber initiatives and, (7) the overall IW program OPSEC level.
- **Sophistication**: (1) the sophistication of the HUMINT program, (2) the overall intelligence capabilities not related to cyber operations and, (3) the capability to remotely delete data from websites or computers.

8. State Control of Private Sector

This node represents the degree to which the private sector has been nationalized or controlled by the state, giving the state control over decisions and operations. Modern computer systems are assembled from components manufactured in various locations, not all of which are tightly controlled. This leads to opportunities for executing a supply chain attack, which is when

> …an attacker disrupts the supply chain lifecycle by manipulating computer system hardware, software, or services for the purpose of espionage, theft of critical data or technology, or to disrupt mission critical operations or infrastructure. Manipulating a technology, component, or product, such as USB thumb drive, digital camera, or digital projector can provide a direct means for compromising targeted organizations with very little risk to the attacker. (Stracener, 2010)

According to the recently released White House Cyberspace Policy Review, “The challenge with supply chain attacks is that a sophisticated adversary might narrowly focus on particular systems and make manipulation

virtually impossible to discover" (Obama, 2011). By exercising control over the private sector, a nation is in position to execute supply chain attacks by influencing the manufacturing process or the logistical chain of the components used later by potential adversaries.

The state control of the private sector node is most heavily influenced by the traits of doctrine, organization, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences state control of the private sector and its support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Doctrine**: (1) the level of state control of the tech sector, (2) the level of state control of the media, (3) the relationships between the government/intelligence organizations and the nation's domestic corporations and, (4) the level of regulation of domestic Internet service providers (ISPs).
- **Organization**: (1) the level of state control of the tech sector and (2) the level of state control of the media.
- **Sophistication**: (1) the level of state control of the tech sector, (2) the level of state control of the media and, (3) a supply chain program.
- **Support to Cyber Operations**: (1) the level of risk to corporations that cooperate with the government on cyber operations and (2) a supply chain program.

B. PRIVATE INDUSTRY

Following government, the next family of nodes is that of the private industry. This node encompasses the research, development and production conducted by the nation's private, or nongovernmental, entities that can be leveraged to develop a sustained, offensive cyber warfare capability. The private industry node has four parent nodes, which are: computer security organizations, network infrastructure, computer hardware companies, and computer software companies (Figure 9). We reasoned that a very important part of a country being able to conduct cyber warfare was whether there were domestic organizations dedicated to the research and development of cyber security best practices, and

domestic corporations dedicated to the development and production of the hardware and software needed to advance the nation's overall IT capability. The presence of these organizations and corporations should provide an indicator of the overall state of cyber maturity. Another factor was the state of the country's network infrastructure (telephone lines, fiber optic lines, Internet service providers, electrical power capacity, etc.). Having a stable network infrastructure is necessary for a cyber warfare capability and the number of the previously mentioned security, hardware and software firms should provide the means for the network infrastructure to grow to support a sustained, offensive cyber warfare capability.

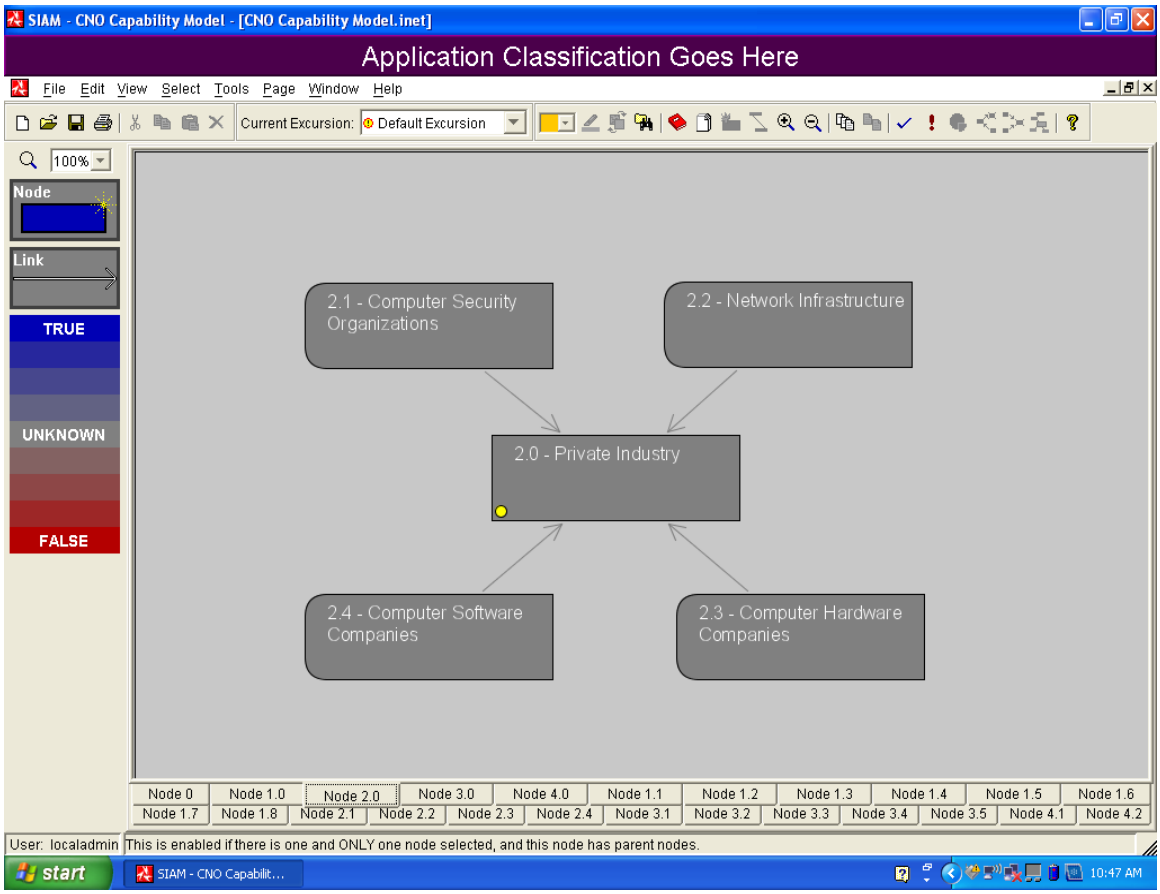

Figure 9. Private Industry node of the Cyber Warfare Capability Model

1. Computer Security Organizations

Before defining what we mean by computer security organizations, we must first define what we mean by computer security itself. Computer security is a subset of information security, which the Federal Information Security Management Act of 2002 defines as, "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability." With this definition in mind, we examined the computer security organizations node as the presence of organizations and companies dedicated to the development and implementation of best practices for guaranteeing the confidentiality, integrity, and availability of the information resident on and transiting computer networks. Included in this node would be traditional anti-virus, computer security companies (i.e., Kapersky Lab and Symantec), not-for-profit computer security organizations (i.e., Team Cymru and the Center for Internet Security), and university affiliated research groups (i.e., Carnegie Mellon's CyLab and Dartmouth College's Institute for Security Technology Studies). This node is designed to encompass the research efforts a country is employing to secure their networks.

The computer security organizations node is most heavily influenced by the traits of training and education, financing, research and development, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences computer security organizations and their support to the overall cyber warfare capability, the analyst should analyze the listed considerations.

- **Training and Education**: (1) relationships with international cyber security organizations, (2) the number of students graduating from cyber security education programs, (3) the number of published articles on cyber security in academic/professional publications and, (4) sponsorship/participation in cyber security conferences.
- **Financing**: (1) the level of state control of the tech sector, (2) gross domestic product (GDP), (3) CND investment and, (4) the relationships between the government/intelligence organizations and the nation's domestic corporations.

- **Research and Development**: (1) the level of state control of the tech sector, (2) sponsorship/participation in cyber security conferences, (3) cyber dedicated facilities, (4) the number of computer security patents, (5) the relationships between the government/intelligence organizations and the nation's domestic corporations, (6) the capability to implement best practices in regards to computer security and, (7) an information security tool development program.
- **Sophistication**: (1) virus proliferation (this would indicate a negative correlation), (2) relationships with international cyber security organizations, (3) the number of published articles on cyber security in academic/professional publications, (4) the number of computer security patents, (5) the capability to implement best practices in regards to computer security and, (6) an information security tool development program.
- **Support to Cyber Operations**: (1) virus proliferation (this would indicate a negative correlation), (2) the number of students graduation from cyber security education programs, (3) the number of computer security patents and, (4) the relationships between the government/intelligence organizations and the nation's domestic corporations.

2. Network Infrastructure

This node represents the capacity of a nation to support the flow of information through the physical hardware used to interconnect computers and users, and includes the transmission media and electrical power capacity. The measures considered in this node represent the whole of a country's information and communications technology capacity. An analyst should consider this node in a similar fashion as INSEAD and the World Economic Forum considered the overall networked readiness index (NRI) in the annual the Global Information Technology Report (Dutta & Mia, 2010). In particular, as part of their environment sub-index, Dutta and Mia considered the infrastructure environment, which was broken down into nine categories, such as the number of telephone lines, the number of secure Internet servers, total Internet bandwidth, etc. Most

of the nine factors are measurable with hard data and widely accessible making an evaluation of the network infrastructure node for the model fairly straightforward.

The network infrastructure node is most heavily influenced by the traits of materiel and facilities. In the model, when determining how each of the traits influences the network infrastructure and its support to the overall cyber warfare capability, the analyst should analyze the listed considerations.

- **Materiel**: (1) the cybercrime level, (2) the scope of the network infrastructure and, (3) the offshoring of computer services (this would indicate a negative correlation).
- **Facilities**: (1) the scope of the network infrastructure, (2) the offshoring of computer services (this would indicate a negative correlation) and, (3) evidence of power needed to support cyber facilities.

3. Computer Hardware Companies

This node represents the nation's domestic corporations that are dedicated to developing the physical components of the computer systems involved in the performance of data processing or communications functions. The Institute of Electrical and Electronics Engineers (IEEE) defines hardware as, "physical equipment used to process, store, or transmit computer programs or data" (IEEE, 1990). These physical components could include processors, memory storage (both hard disk and random access), input devices (keyboards and mice), output devices (displays and monitors), as well as other peripherals (printers, modems, servers, etc.). It is on the hardware that the various applications or programs, known as software, are installed and executed. A nation that has a large number of companies devoted to the development and production of computer hardware would have an advantage over the nations that do not when developing a national network infrastructure.

The computer hardware companies node is most heavily influenced by the traits of materiel, facilities, research and development, and sophistication. In the

model, when determining how each of the traits influences computer hardware companies and their support to the overall cyber warfare capability, the analyst should analyze the listed considerations.

- **Materiel**: (1) the number of computers per person, (2) the number of cyber dedicated facilities, (3) the covert communications capability and, (4) the dependence on the Internet for communications.
- **Facilities**: (1) the number of cyber dedicated facilities, (2) the covert communications capability, (3) the number of domestic ISPs and, (4) the ability to produce high tech, noncyber military equipment.
- **Research and Development**: (1) the level of state control of the tech sector, (2) the number of cyber related facilities, (3) the relationships between the government/intelligence organizations and the nation's domestic corporations and, (4) the ability to produce high tech, noncyber related military equipment.
- **Sophistication**: (1) virus proliferation (this would indicate a negative correlation), (2) the relationships with international cyber security organizations, (3) the covert communications capability, (4) the national connectivity to the global IT infrastructure and, (5) the ability to produce high tech, noncyber military equipment.

4. Computer Software Companies

This node represents the nation's domestic corporations that are dedicated to developing and implementing the applications, drivers, middle-ware, test-ware, programming tools and operating system software that run on the computers, networks and communications systems. The IEEE defines software as "computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system" (IEEE, 1990). It is the software that controls what the computer executes and provides an interface between the computer system hardware and the user—either human or automated. As in the computer hardware companies node, a nation with a large number of companies devoted to the development and implementation of computer software would have a distinct advantage over the countries that do not when developing a national network infrastructure.

The computer software companies node is most heavily influenced by the traits of materiel, research and development, and sophistication. In the model, when determining how each of the traits influences computer software companies and their support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Materiel**: (1) the number of computers per person, (2) the number of cyber dedicated facilities, (3) the covert communications capability and, (4) the ability to produce high tech, noncyber military equipment.
- **Research and Development**: (1) the level of state control of the tech sector, (2) the relationships between the government/intelligence organizations and the nation's domestic corporations, (3) an information security tool development program and, (4) the ability to produce high tech, noncyber military equipment.
- **Sophistication**: (1) virus proliferation (this would indicate a negative correlation), (2) relationships with international cyber security organizations, (3) the covert communications capability, (4) an information security tool development program and, (5) the ability to produce high tech, noncyber military equipment.

C. SCIENCE AND TECHNOLOGY

The next family of nodes is that of science and technology, which considers the state of maturity of a nation's capability in a few highly technical scientific fields, as well as the level of commitment and funding for overall scientific research. The science and technology node has five parent nodes: cryptographic capability, forensic capability, reverse engineering capability, national research laboratories, and other scientific communities (Figure 10). We considered a nation's capabilities in cryptography, computer forensics, and the reverse engineering of electronics as very strong indicators of an overall capability to develop a sustained, offensive cyber warfare program. Cryptography is important for both CNA/E and CND, while computer forensics and reverse engineering require an advanced understanding of computer engineering. These together provide a solid foundation for a country to project a

cyber warfare capability. Also important is the level of commitment the government gives to the research in these and related areas. We considered the U.S. National Laboratory System as a good exemplar. If a country has the ability to bring together the leading scientists in various fields to work together on cutting edge research, then that country could potentially develop the necessary skill sets to field a cyber warfare capability. Another aspect we considered important was the state of maturity in a country's other advanced scientific communities. A country that has advanced scientifically in disciplines other than cyber is much more likely to be able to develop a sustained, offensive cyber warfare capability than those nations that are not.

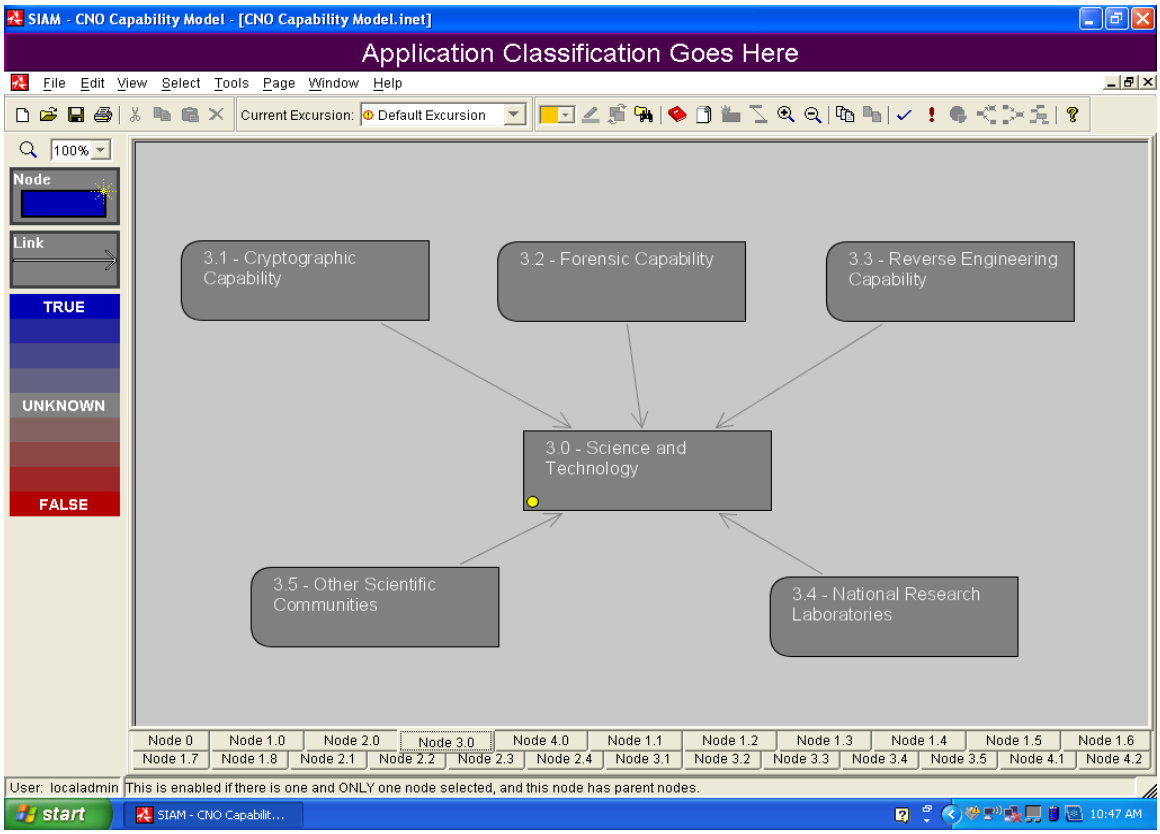

Figure 10. Science and Technology node of the Cyber Warfare Capability Model

1. Cryptographic Capability

This node represents the level at which a country can perform cryptographic and cryptanalytic functions, which can be an indicator of overall IT capability and maturity. Employment of cryptographic functions can be for both defensive and offensive purposes. Defensively, encryption helps safeguard the information resident on particular hosts and data in transit across a network. As long as the secret keys are kept secret, then the data should be secure from unauthorized access. It also important to note that, as stated earlier, there is a strong relationship between a nation's knowledge of how to defend its networks and being able to translate that information into an offensive attack or exploitation capability (Denning, 2007). Offensively, attackers can use cryptanalysis to break the encryption of targeted networks. Additionally, attackers can use encryption to prevent their malicious code from being identified, both during installation and once resident on the targeted computer. One recent example is the W32.Stuxnet worm that as of September 2010 had infected approximately 100,000 computers worldwide, with the highest concentration in Iran. The creators of Stuxnet made extensive use of encryption, particularly of the .dll files, in order to bypass security mechanisms on the targeted computers. Also encrypted was the data Stuxnet sent back to the dedicated, remote command and control servers (Falliere, Murchu & Chien, 2010). An advanced cryptographic capability indicates access to and understanding of advanced computer hardware and software and can be an indicator of a country's cyber warfare capability.

The cryptographic capability node is most heavily influenced by the traits of materiel, research and development, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences the cryptographic capability and its support to the overall cyber warfare capability, the analyst should analyze the listed considerations.

- **Materiel**: (1) the presence of a quantum cryptography program, (2) cyber dedicated facilities, (3) the level of botnet activity and, (4) a ranking in the top 100 of the world's fastest computers.

- **Research and Development**: (1) cyber dedicated facilities, (2) the presence of Silicon Valley-like high tech corridors, (3) the number of computer security patents, (4) the capability to steal technology and make use of it outside of cyber operations, (5) the relationships between the government/intelligence organizations and the nation's domestic corporations, (6) an information security tool development program, and (7) a CNA tool development program.
- **Sophistication**: (1) the presence of a quantum cryptography program, (2) relationships with international cyber security organizations, (3) the midpoint SIGINT capability, (4) the presence of Silicon Valley-like high tech corridors, (5) the number of computer security patents, (6) the role that IO plays across the spectrum of conflict, (7) the use of steganography, (8) the capability to steal technology and make use of it outside of cyber operations, (9) the level of botnet activity, (10) the capability to implement best practices in regards to computer security, (11) an information security tool development program, and (12) a CNA tool development program.
- **Support to Cyber Operations**: (1) the midpoint SIGINT capability, (2) the presence of Silicon Valley-like high tech corridors, (3) the role that IO plays across the spectrum of conflict, (4) a ranking in the top 100 of the world's fastest computers and, a CNA tool development program.

2. Forensic Capability

This node represents the level at which a nation can perform computer forensics, which is a strong indicator of an advanced IT capability. As defined by the United States Computer Emergency Readiness Team (US-CERT), computer forensics is:

> The discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law. (2008)

Being capable of conducting computer forensics provides the advantage of learning specifics about an attacker's methods (tools used, vulnerabilities exploited, data lost, etc.). In his report to the U.S.–China Economic and Security Review Commission, Bryan Krekel detailed how, using forensic techniques, a

U.S. commercial firm was able to re-create an attack scenario that cost the firm large amounts of data (exactly how much still is not known) (2009). Through forensics, the firm's information security staff was able to determine that only specific items of data were exfiltrated, indicating the attackers were working from a specific set of collection requirements. The attackers worked in two distinct teams each employing different toolsets: one team for the breach of the network and one team for the collection and exfiltration of the data. The staff determined the specifics on how the exfiltration took place, even to the point of finding that the collected data was compressed into 650MB files (the maximum capacity of a standard CD-ROM) prior to exfiltration. Most importantly was that although the firm could not definitively ascertain the identity of the attackers, forensics allowed the staff to identify specific keyboard presences. This refers to the specific habits an attacker develops over the course of performing the same functions many times. The sophistication, frequency, combination of commands, and elapsed time between keyboard entries all contribute to defining an individual forensic profile for an attacker. Comparing their forensic profiles to those seen in the past, the staff determined this case was consistent with previous intrusions into U.S. networks by Chinese attackers (Krekel, 2009). An advanced computer forensics capability indicates well-developed knowledge of computer engineering and networks that could readily be applied to the development of a sustained, offensive cyber warfare capability.

The forensic capability node is most heavily influenced by the traits of research and development, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences the forensic capability and its support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Research and Development**: (1) the acquisition of black market cyber tools, (2) cyber dedicated facilities, (3) the capability to steal technology and make use of outside of cyber operations, (4) the relationships between the government/intelligence organizations and the nation's domestic corporations and, (5) a CNA tool development program.

- **Sophistication**: (1) the acquisition of black market cyber tools, (2) the relationships with international cyber security organizations, (3) the presence of Silicon Valley-like high tech corridors, (4) the role that IO plays across the spectrum of conflict, (5) the capability to steal technology and make use of it outside of cyber operations, and (6) a CNA tool development program.
- **Support to Cyber Operations**: (1) the acquisition of black market cyber tools, (2) the presence of Silicon Valley-like high tech corridors, (3) the role that IO plays across the spectrum of conflict and, (4) a CNA tool development program.

3. Reverse Engineering Capability

This node represents the level at which a country can perform reverse engineering, which is a strong indicator of an advance IT capability. The Merriam-Webster dictionary defines reverse engineering as disassembling and examining or analyzing in detail to discover the concepts involved in manufacture in order to produce something similar ("reverse engineering," n.d.). The term also applies to intangible concepts as well, most notably for the model, to software and strings of malware. A country that has the technological know-how to examine in detail the source code of a string of malware used as an exploit has a significant advantage when it comes to engineering their own methods of attack. This reverse engineering capability goes beyond being able to read and implement the results of reverse engineering from the commercial computer security companies and laboratories. Here, the capability refers to whether a particular country has the capability to conduct this type of analysis in-house without relying on others to do it for them. Possessing an advanced reverse engineering capability for software and strings of malware indicates the capacity to develop cyber related exploits for use in a cyber warfare program.

The reverse engineering capability node is most heavily influenced by the traits of research and development, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences the reverse engineering capability and its support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Research and Development**: (1) the acquisition of black market cyber tools, (2) the sophistication of the HUMINT program, (3) cyber dedicated facilities, (4) the capability to steal technology and make use of it outside of cyber operations, (5) the relationships between the government/intelligence organizations and the nation's domestic corporations, (6) an information security tool development program and, (7) a CNA tool development program.
- **Sophistication**: (1) the acquisition of black market cyber tools, (2) the presence of Silicon Valley-like high tech corridors, (3) the role that IO plays across the spectrum of conflict, (4) the capability to steal technology and make use of it outside of cyber operations, (5) the capability to implement best practices in regards to computer security, (6) an information security tool development program and, (7) a CNA tool development program.
- **Support to Cyber Operations**: (1) the acquisition of black market cyber tools, (2) the presence of Silicon Valley-like high tech corridors, (3) the role that IO plays across the spectrum of conflict and, (4) a CNA tool development program.

4. National Research Laboratories

This node represents the presence of government funded and run research laboratories, which can indicate the level of commitment and funding necessary to develop a cyber warfare capability. As a model, we used the United States Department of Energy (DOE) National Laboratory System, encompassing 21 national laboratories and technology centers. Even though they are sponsored by the DOE, these laboratories and technology centers conduct cutting edge research on a variety of scientific and technological topics, including computer science. For example, the mission of the Computer Science and Mathematics Division at the Oak Ridge National Laboratory includes:

> Working on important national priorities with advanced computing systems, working cooperatively with U.S. Industry to enable efficient, cost-competitive design, and working with universities to enhance science education and scientific awareness. Our researchers are finding new ways to solve problems beyond the reach of most computers and are putting powerful software tools into the hands of students, teachers, government researchers, and industrial scientists. (Oak Ridge National Laboratory, 2011)

Another example is Sandia National Laboratory's Science, Technology, and Engineering (ST&E) Mission Area, which includes investment in six research foundations, one of which is computers and information science. The ST&E mission is to create:

> Innovative, science-based, systems-engineering solutions to our Nation's most challenging national security problems. Sandia's guiding principals [sic] for ST&E ensure that the fundamental science and engineering core is vibrant and pushing the forefront of knowledge. Enabling our programs by effective application of that science base allows us to respond to current needs as well as anticipate the future. (Sandia National Laboratories, 2011)

The ability of a nation to bring together the leading scientists in particular fields and fund their research on state-of-the-art technologies is a strong indicator of the overall funding and commitment necessary to develop a sustained, offensive cyber warfare capability if they choose to do so.

The national research laboratories node is most heavily influenced by the traits of research and development, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences the national research laboratories and their support to the overall cyber warfare capability, the analyst should analyze the listed considerations.

- **Research and Development**: (1) the midpoint SIGINT capability, (2) the number of computer security patents, (3) the capability to steal technology and make use of it outside of cyber operations, (4) an information security tool development program and, (5) a CNA tool development program.
- **Sophistication**: (1) the number of computer security patents, (2) the role that IO plays across the spectrum of conflict, (3) the capability to steal technology and make use of it outside of cyber operations, (4) an information security tool development program and, (5) a CNA tool development program.
- **Support to Cyber Operations**: (1) the midpoint SIGINT capability, (2) the number of computer security patents, (3) the role that IO plays across the spectrum of conflict and, (4) a CNA tool development program.

5. Other Scientific Communities

This node represents the presence and maturity of other scientific communities (space or nuclear, etc.). While not directly related to a cyber capability, technical maturity in other advanced scientific communities can indicate that the country had the requisite general scientific knowledge to develop a cyber warfare capability.

The other scientific communities node is most heavily influenced by the trait sophistication. In the model, when determining how each of the traits influences the other scientific communities and their support to the overall cyber warfare capability, the analyst should analyze the following considerations: (1) satellite programs, (2) nuclear programs and, (3) the ability to produce high tech, noncyber related military equipment.

D. ACADEMICS AND RESEARCH

The final node family is that of academics and research. This node focuses on the resources (skilled manpower) that a nation can draw upon, rather than the institutions themselves. Educational institutions and professional organizations facilitate the development of a strong academic and research community. The Academics and Research Node represents the ability of a nation to educate a force of IT professionals to fill roles in the government and private sector and how well connected the educated IT professional are in the international cyber related community. This node is composed of two parent nodes, which are an educated force and affiliation with professional organizations (Figure 11). The intent here was to create a separate category from the research being conducted by the private sector (as analyzed in the private sector node family) with the emphasis primarily on the academic aspect. We saw the most important factor here being the educated force, not just those already educated and working in a cyber related field, but also those being educated in cyber and representing the next generation of cyber operators. Also considered was the degree to which a county's IT professionals affiliate with professional cyber

related organizations. A large number of affiliations would indicate that country's professionals are respected and have access to the current international research and development efforts that can be leveraged in their own cyber education programs.

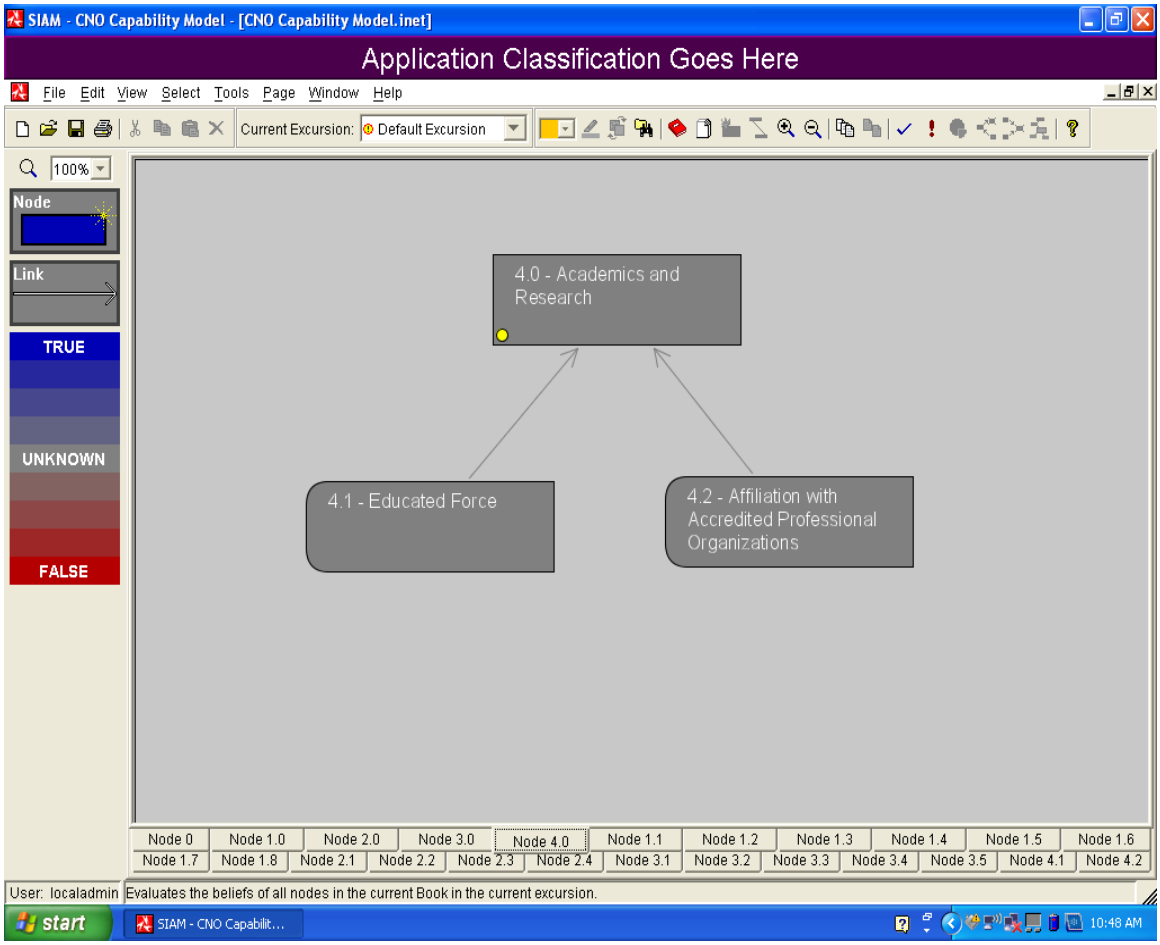

Figure 11. Academics and Research node of the Cyber Warfare Capability Model

1. Educated Force

This node represents the number of people who are educated in the disciplines of computer science/security/engineering. An educated force would consist of individuals working in a variety of environments, including government, the private sector, and academia. Those working in government could be applied directly to the cyber warfare mission, while those working in the private

sector could be involved in the research and development aspect of a cyber warfare mission. Perhaps more importantly, would be those working in academia, educating a steady stream of cyber-capable graduates who go on to work in either the government or private sectors. It is these graduates and working IT professionals who make possible the cryptographic, forensic, and reverse engineering capabilities, as well as being directly employed as cyber operators for the state. A country with large numbers of educated IT professionals has a large pool from which to draw in order to develop and sustain a cyber warfare capability.

The educated force node is most heavily influenced by the traits of training and education, personnel, and sophistication. In the model, when determining how each of the traits influences the educated force and its support to the overall cyber warfare capability, the analyst should examine the listed considerations.

- **Training and Education**: (1) linguistic capability, (2) the number of computer security students studying abroad, (3) GDP, (4) the number of cyber based research publications, (5) the number of students graduating from cyber security education programs, (6) the number of published articles on cyber security in academic/professional publications, (7) the recruiting of students to act as cyber operators, (8) the pervasiveness of computer science/computer engineering programs and, (9) the offshoring of computer services (this would indicate a negative correlation).
- **Personnel**: (1) the number of students graduating from cyber security education programs, (2) the number of cyber related contracts for bid and, (3) the offshoring of computer services (this would indicate a negative correlation).
- **Sophistication**: (1) the presence of a quantum cryptography program, (2) the number of cyber based research publications, (3) the number of computers per person, (4) the technological sophistication of the population, (5) the number of computer security patents and, (6) the use of steganography.

2. Affiliation with Professional Organizations

A country with large numbers of IT professionals who are affiliated with accredited, professional cyber-related organizations (ACM, IEEE, ISSA, etc.) can

draw from a pool of people who are educated, professional, networked, and are familiar with the state-of-the-art and best practices of cyber-related disciplines. While not necessarily a direct indication of a cyber warfare capability, the number of IT professionals affiliated with respected cyber-related organizations can provide an indication of the state of a country's IT sector maturity. Affiliation with these organizations allows access to up-to-date technological information on computer and communication systems from both an engineering (hardware, software, and systems engineering) and operational (computer network attack and defense) perspective. A potentially strong indication of the IT sector maturity is how often researchers from a particular country publish articles in scholarly journals and other periodicals associated with these professional organizations.

The affiliation with professional organizations node is most heavily influenced by the traits of training and education, sophistication, and support to cyber operations. In the model, when determining how each of the traits influences the affiliation with professional organizations and its support to the overall cyber warfare capability, the analyst should analyze the listed considerations.

- **Training and Education**: (1) the number of memberships in IT related groups (i.e., IEEE, ACM, ISSA), (2) the number of cyber related research publications and, (3) sponsorship/participation in cyber security conferences.
- **Sophistication**: (1) the number of memberships in IT related groups (i.e., IEEE, ACM, ISSA), (2) the relationships with international cyber security organizations, (3) sponsorship/participation in cyber security conferences and, (4) diplomatic cyber initiatives.
- **Support to Cyber Operations**: (1) the number of memberships in IT related groups (i.e., IEEE, ACM, ISSA), (2) the number of cyber based research publications, (3) the relationships with international cyber security organizations and, (4) access to computer security data from international organizations (INTERPOL, ITU, etc.).

V. CONCLUSION AND RECOMMENDATIONS

Thesis conclusions are articulated, followed by key recommendations that could improve the SIAM Cyber Warfare Capability Model.

A. CONCLUSIONS

This thesis explored a new approach to examining whether a country possesses a sustained, offensive cyber warfare capability. In doing so, we attempted to identify a process to quantify the baseline information needed to model a complex problem allowing analysts to understand the reasoning behind the assessments made by the model. The SIAM Cyber Warfare Capability Model is meant to be used as a mechanism to examine in detail the factors that should indicate a country's cyber warfare capabilities.

The culmination of our work, the Cyber Warfare Capability Model, was delivered to the sponsor, who then shared the model with other agencies involved with identifying, analyzing, and tracking countries that possess a sustained, offensive cyber warfare capability. The sponsor said the modified DOTMLPF Analysis in our model provided a solid foundation for future modeling efforts.

The sponsor's vision for the model had changed from the requirements laid out for our initial effort. The sponsor initially envisioned assessing whether a country has the capability to conduct sustained, offensive cyber warfare using a strictly resources-based approach. The sponsor expressed that the modified DOTMLPF Analysis employed in the Cyber Warfare Capability Model did an excellent job of accounting for a resources methodology. However, the sponsor decided to look at the problem from a different perspective within a framework that connected the different offensive cyber missions with different operations in addition to resources. The sponsor built a model in SIAM, the State Offensive Cyber Program Capabilities Model, taking a capability equals sophistication

times resources approach. The sponsor used our model and methodology to account for resources and inform the various intelligence services. We felt that the incorporation of our model and methodology into the State Offensive Cyber Program Model was validation for our work and the approach employed.

We used a systems engineering approach, incorporating a modified DOTMLPF Analysis, to view a country's cyber warfare capability. The top-down approach allowed us to transform the sponsor's initial requirements into a viable solution. The sponsor said the systematic process employed in our model accounted for a resource based approach and met the design goals initially laid out. The Cyber Warfare Capability Model is a novel approach and hopefully will provide a launching point to start understanding state offensive cyber programs.

B. RECOMMENDATIONS

The model presented in this thesis met the initial expectations, as it does an excellent job of accounting for a resource-based approach to assess the sustained, offensive cyber warfare capabilities of a country. However, certain aspects should be taken into consideration for future research and validation of the model.

1. Complexity

SIAM is designed to assess very complex issues. However, one must remember the user in the process of designing a model. If the model becomes too complex, the user may not be able to gain any benefit from it. We felt that the current model did a fairly good job of keeping thoughts organized in a hierarchal manner, despite the 15,010 (190 traits x 79 considerations) evaluations required to develop the model. In our opinion, once our model was combined into the State Offensive Cyber Program Model, it lost the simplistic hierarchal approach. It was not necessarily self-apparent which nodes were the Initial Nodes, requiring user input. This is something that can be remedied, but

must be kept in mind when creating a user-friendly model. The analysts' ability to use the model as a tool is the ultimate litmus test.

During the development of the model, we constrained ourselves to work within the data given to us by the sponsor (object, traits, and considerations). We think this limitation was beneficial for the initial development as it limited the scope of our thinking and research. It also allowed us to focus on building a hierarchical model where the inputs required by the analyst were apparent. However, after going through the process of developing and analyzing our completed model, we have come to the conclusion that the model could be greatly simplified, while still maintaining the same functionality. While the modified DOTMLPF Analysis provided an excellent framework for thinking about state sponsored cyber programs, it also proved to be quite redundant. We believe the model does a very good job of accounting for the problem, but may be overly complex. In order to facilitate a more user friendly model, we have identified a few suggestions for consideration by the sponsor.

First, within the government node family, we would suggest combining the four separate intelligence services nodes (domestic, foreign, signals, and military) into a single node. While it was useful for us to view these intelligence services individually, it created a large amount of redundancy when analyzing the considerations that inform the traits for each intelligence service. For a more user friendly model, these could be combined into a single node representing the country's overall intelligence capability so that the analyst would only need to examine intelligence once. Doing this would decrease the number of intelligence-related traits that need input from the analyst by 75%.

The second suggestion is to combine the two node families of private sector with academics and research into a single node family that would encompass the research and development efforts by a country. While our model accounts for the research and development in two separate sectors, it is hard to separate the research communities since the researchers in both attend the same conferences and often publish in the same places. In fact, people in

academia and industry coauthor many papers and many PHDs go into the private sector where they continue their research. In retrospect, there may be very little value added from analyzing this with two distinct node families.

Our third suggestion is to redefine the trait categories we used for our modified DOTMLPF analysis. In our model, we used ten categories of traits, but these could be simplified by combining the ten traits into four broader categories. For example, our traits of organization, training and education, and personnel and manpower could be combined into a single trait of personnel used by the analyst to consider the information previously needed to inform the three traits. Additionally, our traits of materiel, financing, and facilities could be combined into a single trait for resources that would encompass the three previously used traits. Finally, we used the traits of sophistication and support to cyber operations, but these really just speak directly to a country's capabilities. For simplicity, these two traits could be combined into a single trait called capabilities and would retain the same functionality. By redefining the categories of traits and simplifying them from ten to four, this would save the analyst 60% of effort across the entire model and would significantly reduce redundancy as well.

Our final recommendation would be to reevaluate the list of considerations used to inform the traits discussed above. The considerations used in the model were an attempt to capture the direct and indirect influences. Each consideration's applicability was deliberated for each trait of the modified DOTMLPF analysis. The resulting model included indirect influences to the traits, which may themselves have a minimal impact on the objects they are informing. The consequence of this is an unnecessarily complicated model that could waste valuable resources and man-hours. The model was conceived in a systemized manner, but this led to many tangible, quantifiable indicators to be accounted for multiple times in an abstract fashion. We think the model would benefit greatly from disregarding the list of considerations altogether. Instead, since the traits are the nodes that require user input, the user can define his or her own set of considerations on a trait-by-trait basis. By eliminating the

constraint of having to pick from a list of predefined considerations, the analyst can eliminate much of the redundancy and ultimately provide a much higher level of fidelity for the overall model.

2. Future Research

Any modeling tool is only as good as the data provided to the model by the user. While our final recommendation above is to get rid of the constrained list of original considerations, we still feel that having a list of things an analyst could consider would be helpful, thus subject matter expert input would greatly benefit this process. A survey to garner expert opinions to compile a general list of considerations for each trait (policy, personnel, resources, and capabilities) could facilitate this. The purpose of the survey would not be to design the list of considerations that an analyst must use, but instead, provide a listing of potential items of interest that the user could consider to help stimulate thought. From this, the user could define which particular considerations to use based on how he or she sees the situation. The ultimate goal is to provide analysts a tool that helps baseline a country's cyber warfare capabilities.

While the methodology was endorsed and incorporated by the sponsor into another, larger, model, the Cyber Warfare Capability Model should go through extensive test scenarios to evaluate the true functionality. Test cases to ensure the results are consistent with the expected results, using disparate examples, would further validate this methodology. Analysis of these test cases could also identify pressure points, applicable across the entire spectrum of countries, and help focus limited resources when modeling is not applicable. This model or even a modified version of it needs to be tested to explore its full potential.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

LIST OF 79 POTENTIAL CONSIDERATIONS

1 Number of Intelligence bases Internationally
2 Level of State control of the Tech sector
3 Membership in IT (IEEE) like groups
4 Acquisition of black market tools
5 Satellite programs
6 Relationships with other cyber actors
7 Linguistic capabilities
8 Size of the hacker community
9 Nuclear capabilities
10 Quantum Crypto program
11 Sophistication of HUMINT program
12 Number of Computer Security Students studying abroad
13 IO Range infrastructure
14 Virus proliferation
15 Strength of Nationalism in population
16 Cyber crime level
17 Level of control of State/private media
18 GDP
19 Cyber based research publications
20 Relationships with international cyber security organizations
21 Number of students graduating from Cyber Security Education programs
22 Number of publications on cyber security in academic publications
23 Midpoint signals intelligence capabilities
24 Sponsorship/participation of cyber security conferences
25 Military spending
26 Network infrastructure
27 Number of computers/person
28 Technological sophistication of the population
29 Cyber dedicated facilities
30 Silicon Valley like high tech corridors
31 Intelligence budget
32 Number of computer security patents
33 Number of cyber related contracts for bid (green badgers)
34 Recruiting of students to act as cyber operators
35 Role that IO plays across the spectrum of conflict
36 Use of offensive computer operations to support programs outside of strategic IW
37 Use of steganography
38 Covert communications capabilities
39 Capability to "steal" technology and make use of it outside of cyber operations
40 Botnet activity
41 CND investment

42 Pervasiveness of computer science /engineering programs
43 Relationships between government/intelligence organizations and the nation's domestic corporations
44 Open source reorganizations of IO organizations
45 National connectivity to global IT infrastructure
46 Covert cyber activity detected
47 Number of domestic ISPs
48 Observation of traveling Govt IT techs servicing IO platforms abroad
49 Overall Intelligence collection capabilities not related to cyber operations
50 Capability to remotely delete data from websites/computers
51 CNA release authority
52 Capability to implement best practices in regard to computer security
53 Capability to create and run front companies
54 Clandestine infrastructure for remote operations
55 Number of classified networks in Govt IT
56 Declaratory response policy
57 Network mapping program
58 CNE success
59 Dependence on for communications
60 Offshoring of computer services (negative correlation)
61 Evidence of storage for massive amount of collected cyber data
62 Evidence of power needed to support cyber facilities
63 Evidence of Internet monitoring program
64 Level of regulation of domestic ISPs
65 Critical infrastructure protection program
66 Info sec tool development
67 Ranking in top 100 of world's fastest computers
68 access to computer security data from international organizations (Interpol, ITU, etc.)
69 Ability to produce high tech noncyber military equipment
70 Operations against domestic opposition websites
71 Risk to corporations that cooperate with Govt on Cyber operations
72 Level of concern over cyber crime
73 Cyber training programs in military/intel services
74 Tech savvy individuals serving in senior Govt positions
75 Diplomatic cyber initiatives
76 IW program OPSEC level
77 Tool development program
78 Supply chain program
79 Undersea cable operations capability

APPENDIX B

MAPPING CONSIDERATIONS TO NODES

Nodes	**1.1**	**1.2**
	Domestic Intel Service	**Foreign Intel Service**
Doctrine, Policy, Legal	2, 43, 70, 72, 76	6, 15, 43, 46, 75, 76
Organization	73, 74	51, 54, 73, 74
Training and Education	73	73
Materials	38, 55	38, 48, 54, 55, 61
Financing	31	31
Facilities	23, 38, 53, 55	1, 23, 38, 54, 55, 61
Personnel/Manpower	33, 74	7, 8, 15, 33, 48, 74
Research and Development	4, 39, 43	4, 39, 43
Sophistication	4, 11, 23, 38, 39, 49, 50	4, 11, 23, 38, 39, 49, 50, 58, 79
Support to Cyber Operations	4, 23, 43, 50	4, 8, 11, 23, 43, 46, 48, 50, 58, 75, 79

Nodes	**1.3**	**1.4**
	Signals Intel Service	**Military Intel Service**
Doctrine, Policy, Legal	2, 6, 35, 36, 43, 46, 70, 75, 76	76
Organization	13, 51, 54, 63, 73, 74	73, 74
Training and Education	13, 73	73
Materials	13, 38, 40, 48, 54, 55, 61, 67	55, 61, 62
Financing	22, 25, 31	25, 31
Facilities	1, 13, 23, 28, 38, 54, 55, 61	1, 23, 55, 61, 62
Personnel/Manpower	33, 48, 74	7, 33, 74
Research and Development	4, 13, 39, 43	4
Sophistication	4, 13, 23, 30, 36, 38, 39, 49, 50, 58, 79	4, 11, 23, 49
Support to Cyber Operations	4, 13, 23, 30, 35, 43, 46, 48, 50, 57, 58, 63, 67, 75, 79	4, 11, 23, 75

Nodes	1.5	1.6
	Cyber Focused Command	Homeland Sec. Network Def.
Doctrine, Policy, Legal	6, 15, 24, 35, 36, 46, 56, 70, 75, 76	6, 16, 20, 24, 52, 68, 75, 76
Organization	13, 44, 51, 54, 73, 74	13, 44, 63, 65, 74
Training and Education	13, 24, 73	13, 22, 24
Materials	13, 48, 54, 55	13, 48, 52, 55
Financing	25, 31, 41	31, 25, 41
Facilities	13, 28, 54, 55, 62	13, 28, 55, 62
Personnel/Manpower	15, 33, 34, 48, 73, 74	33, 34, 48, 74
Research and Development	4, 13	13, 41
Sophistication	4, 13, 36, 58	13, 14, 52
Support to Cyber Operations	4, 8, 13, 24, 35, 46, 48, 58, 75	13, 24, 48, 63, 75, 76

Nodes	1.7	1.8
	Law Enforcement	State Ctrl. Priv. Sector
Doctrine, Policy, Legal	6, 16, 68, 70, 72, 75, 76	2, 43, 64
Organization	74	2, 17
Training and Education	x	x
Materials	x	x
Financing	x	x
Facilities	x	53
Personnel/Manpower	74	x
Research and Development	x	x
Sophistication	11, 49, 50	2, 78
Support to Cyber Operations	50, 75	71, 78

Nodes	2.1	2.2
	Computer Sec. Org.	Network Infrastructure
Doctrine, Policy, Legal	71	64
Organization	x	2, 59
Training and Education	20, 21, 22, 24	x
Materials	29, 52	16, 26, 60
Financing	2, 18, 41, 43	18
Facilities	29	26, 60, 62
Personnel/Manpower	21, 29, 42	x
Research and Development	2, 24, 29, 32, 43, 52, 66	x
Sophistication	14, 20, 22, 32, 52, 66	2
Support to Cyber Operations	14, 21, 32, 43	x

Nodes	2.3	2.4
	Computer Hardware Companies	Computer Software Companies
Doctrine, Policy, Legal	71	71
Organization	x	x
Training and Education	20	20
Materials	27, 29, 38, 59	27, 29, 38, 69
Financing	2, 18, 43	2, 18, 43
Facilities	29, 38, 47, 69	38, 69
Personnel/Manpower	29, 42	42
Research and Development	2, 29, 43, 69	2, 43, 66, 69
Sophistication	14, 20, 38, 45, 69	14, 20, 38, 66, 69
Support to Cyber Operations	43, 78	14, 43, 78

Nodes	3.1	3.2
	Cryptographic Capability	Forensics Capability
Doctrine, Policy, Legal	59	x
Organization	x	x
Training and Education	20	20
Materials	10, 29, 40, 67	29
Financing	43	43
Facilities	29	29
Personnel/Manpower	29, 42	29, 42
Research and Development	29, 30, 32, 39, 43, 66, 77	4, 29, 39, 43, 77
Sophistication	10, 20, 23, 30, 32, 35, 37, 39, 40, 52, 66, 77	4, 20, 30, 35, 39, 77
Support to Cyber Operations	23, 30, 35, 67, 77	4, 30, 35, 77

Nodes	3.3	3.4
	Reverse Engineering	NRL
Doctrine, Policy, Legal	x	x
Organization	x	x
Training and Education	x	x
Materials	29	x
Financing	43	x
Facilities	29	x
Personnel/Manpower	29, 42	42
Research and Development	4, 11, 29, 39, 43, 66, 77	23, 32, 39, 66, 77
Sophistication	4, 30, 35, 39, 52, 66, 77	32, 35, 39, 66, 77
Support to Cyber Operations	4, 30, 35, 77	23, 32, 35, 77

Nodes	3.5
	Other Scientific Communities
Doctrine, Policy, Legal	x
Organization	x
Training and Education	x
Materials	69
Financing	x
Facilities	69
Personnel/Manpower	42
Research and Development	69
Sophistication	5, 9, 69
Support to Cyber Operations	5

Nodes	4.1	4.2
	Educated Force	**Affiliation w/ Professional Orgs.**
Doctrine, Policy, Legal	x	x
Organization	x	x
Training and Education	7, 12, 18, 19, 21, 22, 34, 42, 60	3, 19, 24
Materials	27	x
Financing	18	x
Facilities	42	x
Personnel/Manpower	21, 33, 60	x
Research and Development	x	24
Sophistication	10, 19, 27, 28, 32,37	3, 20, 24, 75
Support to Cyber Operations	19, 21	3, 19, 20, 68

APPENDIX C

CNO CAPABILITY MODEL GUIDE

I. Overview

The SIAM Cyber Warfare Capability Model is analytical tool based on Causal Strengths (CAST) Logic to determine the capability of a nation state to conduct sustained, offensive cyber operations. CAST Logic is based on Bayesian mathematics, which allows for the evaluation of the cumulative effect that multiple causes may have on a single event. The analyst is able to enter the confidence level of the information contained in the node, as well as the corresponding influence on the connecting node. The analyst is also able to alter the information contained in the node along with the strength of the link, as more information is made available. This provides for a readily updateable model that considers multiple indicators and relationships.

II. Model

The Cyber Warfare Capability Model is a four level model in which the analysts will inform nodes at the lowest level and define the relationships (links) between all nodes. The analyst inputs data to inform the Level 4 nodes, which inform the level 3 nodes (Figure 12) and so on in a bottom up fashion. The belief level of the nodes at levels 1, 2, and 3 will be computed from the causal relationships that influence them.

A. Informing Nodes

The analyst double clicks the desired Level 4 Node and defines the current belief of the node using a slide bar. The analyst forms this decision based on the informing considerations presented in the comments tab. The analyst is able to document and hyperlink source material under the Sources and Library tab. The analyst can disregard nodes if information is not available by leaving the current belief as unknown.

B. Defining Links

The analyst must define all links in the model. The analyst double clicks the links and uses a slide bar to define the impact of the nodes if the premise is true or false. This property allows the analyst to define whether it is a negative or positive relationship. The model is largely based on positive relationships, therefore if the analysts defines a negative relationship it needs to be a conscious decision and properly reflected with the slide bar and comments.

C. Run the Model

The analyst clicks the exclamation mark in the upper right hand corner to run the model (belief evaluation). The three tabs to the right of the exclamation mark provide impact analysis and pressure point evaluations.

III. Summary

The Capability Model may identify "key inputs" among all the selectors. This could be very useful in focusing the analyst on important information that deserves more attention than other factors. The analysts should emphasize efforts towards defining relationships to this effect.

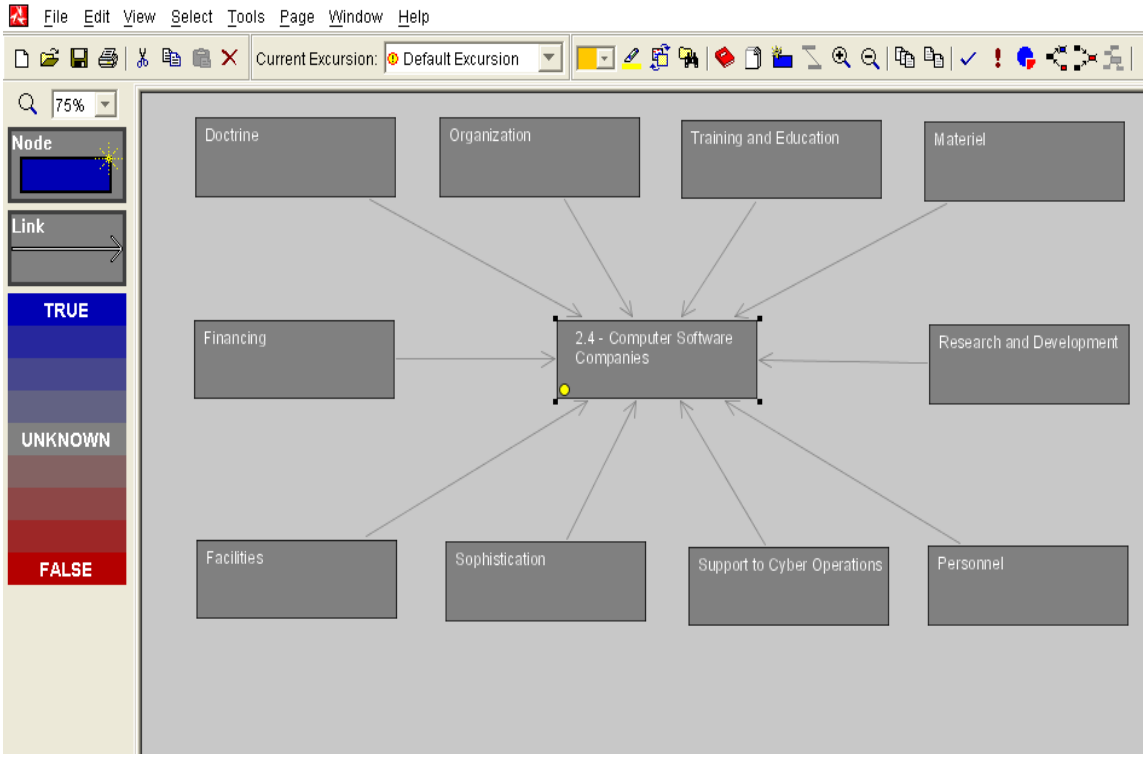

Figure 12. Level 4 nodes informing level 3 node

The Level 4 Nodes (Doctrine, Organization, etc.) represent the traits of the Level 3 Node. It is the Level 4 Nodes that represent the modified DOTMLPF analysis used to inform the Level 3 Nodes and that is where the analyst will input the data for the particular country of interest.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Billo, C. & Chang, W. (2004). *Cyber warfare: Ann analysis of the means and motivations of selected nation states*. Hanover, NH:Dartmouth College.

Chairman of the Joint Chiefs of Staff. (2011, March 7). *Joint Capabilities integration and Development System*. Retrieved August 5, 2011, from www.dtic.mil:http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170.01.pdf

Cyberwar: War in the fifth domain. (2010, July 1). *The Economist.* Retrieved July 20, 2011, http://www.economist.com/node/16478792

Denning, D. E. (2007). Assessing the computer network operations threat of foreign countries. In J. Arquilla & D. A. Borer (Eds.), *Information strategy and warfare: A guide to theory and practice* (pp. 187–210). New York: Routledge.

Department of Defense. (2011). *Joint publication 1-02, dictionary of military and associated terms.* Washington, DC: Joint Chiefs of Staff.

Dutta, S., & Mia, I. (2010). *Global information technology report 2009-2010: ICT for sustainability.* Geneva: World Economic Forum.

FBI warns brewing cyberwar may have same impact as 'well-placed bomb.' (2010, March 8). Fox News. Retrieved July 20, 2011, from http://www.foxnews.com/scitech/2010/03/08/cyberwar-brewing-china-hunts-wests-intel-secrets/

Falliere, N., Murchu, L. O., & Chien, E. (2010). *W32.Stuxnet dossier, version 1.3.* Cupertino: Symantec Security Response.

Federal Bureau of Investigation. (n.d.). *FBI intelligence philosophy*. Retrieved July 18, 2011, from FBI.gov: http://www.fbi.gov/about-us/intelligence/philosophy

Federal Information Security Management Act of 2002, 44 U.S.C. §3542 (2002).

Institute of Electrical and Electronics Engineers. (1990). *IEEE standard computer dictionary*. New York: Author.

Johnston, R. (2005). *Analytic culture in the U.S. intelligence community: An ethnographic study.* Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence.

Krekel, B. (2009). *Capability of the People's Republic of China to conduct cyber warfare and computer network exploitation.* McLean, VA: Northrop Grumman.

Oak Ridge National Laboratory. (2011, June 23). *CSM: Computer Science and Mathematics Division*. Retrieved August 2, 2011, from: http://www.csm.ornl.gov/

Obama, Barack. (2011). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure.* Washington, DC: The White House.

Pellerin, C. (2010, October 18). *Lynn: cyberspace is the new domain of warfare*. Retrieved July 20, 2011, from Defense.gov: http://www.defense.gov/news/newsarticle.aspx?id=61310

Reverse engineering. (n.d.). In Merriam-Webster's online dictionary. Retrieved August 2, 2011, from http://www.merriam-webster.com/dictionary/reverse%20engineering

Rosen, J. A. & Smith, W. L. (1996). *Influence net modeling with causal strengths: An evolutionary approach.* McLean, VA: Science Applications International Corporation.

Rosen, J. A. & Smith, W. L. (1996, Summer). *Influencing global situations: A collaborative approach*. McLean, VA: Science Applications International Corporation.

Sandia National Laboratories. (2011). *Sandia National Labs mission areas: Science, technology and engineering*. Retrieved August 2, 2011, from: http://www.sandia.gov/mission/ste/

Stracener, T. (2010, December 1). *CAPEC-437: Supply chain attacks*. Retrieved July 21, 2011, from capec.mitre.org: http://capec.mitre.org/data/definitions/437.html

Science Applications International Corporation (1995). *Situational Influence Assessment Module, user's manual version 6.0*. McLean, VA: Author.

United States Computer Emergency Readiness Team. (2008). *Computer forensics.* Retrieved August 3, 2011, from US-CERT website: http://www.us-cert.gov/reading_room/forensics.pdf

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Raymond Buettner
   Naval Postgraduate School
   Monterey, California

4. Dorothy Denning
   Naval Postgraduate School
   Monterey, California

5. D.C. Boger
   Naval Postgraduate School
   Monterey, California